STOPPING SPAM

CREATING A STRONGER, SAFER INTERNET

Report of the Task Force on Spam
May 2005

Canada

STOPPING SPAM

CREATING A STRONGER, SAFER INTERNET

Report of the Task Force on Spam
May 2005

This publication is available upon request in multiple formats.
Contact the Information Distribution Centre at the numbers listed below.

For additional copies of this publication, please contact:

Information Distribution Centre
Communications and Marketing Branch
Industry Canada
Room 268D, West Tower
235 Queen Street
Ottawa ON K1A 0H5

Tel.: (613) 947-7466
Fax: (613) 954-6436
Email: **publications@ic.gc.ca**

This publication is also available electronically on the World Wide Web at the following address:
www.e-com.ic.gc.ca

Permission to Reproduce
Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from Industry Canada, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that Industry Canada is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced, nor as having been made in affiliation with, or with the endorsement of, Industry Canada.

Opinions and statements in the publication attributed to named authors do not necessarily reflect the policy of Industry Canada or the Government of Canada.

For permission to reproduce the information in this publication for commercial redistribution, please email:
copyright.droitdauteur@pwgsc.gc.ca

Cat. No. Iu64-24/2005
ISBN 0-662-68997-6
514279B

Cover: 10%
Inside pages: 10%

May 2005

The Honourable David L. Emerson, P.C., M.P.
Minister of Industry
5th Floor, West Tower
235 Queen Street
Ottawa, Ontario K1A 0H5

Dear Minister:

On May 11, 2004, the Government of Canada announced the launch of *An Anti-Spam Action Plan for Canada* and established a government–private sector task force to oversee and coordinate its implementation. We were given one year to do this work. At the end of this period, we were asked to report on the progress made, and to propose any new actions that might be required.

We are pleased to report that we were able to make significant progress toward the goal of stopping spam. This was only possible because of the assistance we received from a large number of people, representing all stakeholder groups, who contributed to our work.

Although we began as a committee of 10 people meeting in a room in Ottawa, we quickly grew to become a network that spanned the country and reached beyond its borders. Much of our work was done online through email. The experience brought home to all of us the potential of the Internet for transforming the ways things get done — and the need to get rid of spam and other threats to Internet use.

Our mandate is finished, but much remains to be done. Our experience has taught us that spam is but one of a number of threats to the safety and security of the Internet as a platform for communications and commerce. We have recommended a series of actions that will help combat spam and spam-related threats in Canada. These actions will position our country as a leader in combatting a growing, worldwide problem. With its long history of leadership in communications, we believe that Canada should aim for nothing less.

Sincerely,

Lori Assheton-Smith

Michael Binder (Chair)

Tom Copeland

Bernard Courtois

Michael Geist

Amanda Maltby

Suzanne Morin

Geneviève Reed

Neil Schwartzman

Roger Tassé

CONTENTS

Letter of Transmittal iii

Executive Summary 1

Recommendations 3

1. Drawing the Line 7
2. Clarifying the Rules 10
3. Managing Networks to Stop Spam 16
4. Restoring Confidence in Email 20
5. Promoting Public Awareness 24
6. Addressing a Global Problem 27
7. Coordinating Future Action 30

Appendices

A. Members of the Task Force Working Groups and Secretariat 33

B. Recommended Best Practices for Internet Service Providers and Other Network Operators 37

C. Recommended Best Practices for Email Marketing 43

D. Three Key Tips for Combatting Spam 50

E. Background Reports and Working Documents 53

Glossary 55

EXECUTIVE SUMMARY

WHAT IS SPAM AND WHY IS IT A PROBLEM?

The May 2004 Anti-Spam Action Plan for Canada defined spam as "unsolicited commercial email." By this definition, the firm MessageLabs estimated that spam accounted for as much as 80 percent of global email traffic at the end of 2004 — up from about 10 percent in 2000.

Spam is more than a growing nuisance. It is a public policy issue that challenges governments, Internet service providers (ISPs), other network operators, commercial emailers and consumers to work together in new ways — with each stakeholder group fully playing its part — to solve a problem that threatens the interests of all.

At the macro level, spam is a direct threat to the viability of the Internet as an effective means of communication. Because of this, spam is also a direct threat to increasing economic prosperity, to more efficient public services and to the emergence of an e-economy that includes all Canadians.

At the micro level, spam annoys and offends Internet users. It also provides a vehicle for activities that are clearly illegal — or should be. These include:

- malicious actions that cause harm to computers, networks or data, or use personal property for unauthorized purposes (e.g. viruses, worms, Trojan Horses, denial of service attacks, zombie networks);
- deceptive and fraudulent business practices, including online versions of traditional mail-based frauds (e.g. the "Nigerian bank account" or "419" scam, and "spoofed" websites masquerading as legitimate businesses);
- phishing emails designed for identity theft or to steal money; and
- invasions of privacy (e.g. email-address harvesting, spyware).

Who Does Spam Hurt?

Because of the above threats, spam undermines consumer confidence in e-commerce and electronic transactions between citizens and their governments. In addition, it imposes significant costs throughout the economy.

These costs fall on a wide range of actors, including:

- ISPs and other network operators (e.g. large enterprise users, universities, government departments), who must invest in the technical, financial and human resources needed to deploy anti-spam technologies, at the expense of investments in new or improved services, and who must allocate resources to respond to customer complaints;

- legitimate commercial emailers and other users of email services whose messages get filtered out by anti-spam technologies before they reach their intended recipients; and
- private and public sector organizations, whose employees waste time dealing with spam sent to their business email addresses.

Ultimately, all of these costs fall directly or indirectly on consumers and Internet end-users, who must cover the costs of fighting spam not only by purchasing Internet security software, but also by foregoing other kinds of service improvements and paying higher prices for online products.

What Do We Need to Do to Fight Spam?

To fight spam, Canada needs to pursue a multifaceted strategy that involves all stakeholders. The Government of Canada's May 2004 Anti-Spam Action Plan was a good beginning. It identified the main tools that are needed to stop spam. These are:

- vigorous enforcement of current laws that prohibit spamming activities, as well as new legislation as required to fill any gaps identified in existing laws;
- stronger penalties and enforcement mechanisms to deter spammers more effectively;
- industry standards and recommended practices to guide ISPs, other network operators and commercial email marketers in the legitimate conduct of business;
- public education and awareness; and
- international cooperation to fight spam.

During the past year, the Task Force on Spam led the development of a unique, made-in-Canada approach to combatting spam, with the assistance of hundreds of people representing different stakeholder groups. This report details the actions the Task Force has taken, and the work that remains to be done. Through the process, the Task Force learned a number of lessons that are important for the ongoing fight against spam, not only in Canada, but also around the world.

The Need for a Multifaceted, Multistakeholder Approach

The most important lesson has been that a multifaceted, multistakeholder approach to fighting spam works — and is the only approach likely to be fully effective in the long term.

Some countries have chosen to fight spam by relying mainly on legislation and regulations to do the job. The Task Force's experience has confirmed that clear laws, strong penalties and vigorous enforcement are needed to fight spam successfully. Our work has also shown that there are gaps in current Canadian law that must be filled, and weaknesses in its enforcement system that must be addressed. Nevertheless, while good legal tools are needed to fight spam, they are not enough to guarantee victory.

Sound business practices, consumer awareness, public education and international cooperation are equally important instruments of the anti-spam toolkit. To maximize results, these tools must be developed and used in a coordinated fashion within a sound legal framework backed by effective enforcement.

The Need for Communication and Cooperation Among Stakeholders

The second major lesson that the Task Force has learned is the importance of getting the different stakeholder groups that are involved in the fight against spam talking and working together.

When the Task Force began its work, we quickly discovered that the structure of the stakeholder community was like a collection of silos within silos, which presented the challenge of bridging the gaps that normally exist between government, the private sector and public-interest advocates because of differences in interests and perspectives.

The experience of working together on practical tasks to fight spam proved to be a very effective way of breaking down these kinds of barriers. As well as improving communications, the multistakeholder approach adopted by the Task Force

produced very significant results in terms of precedent-setting anti-spam enforcement actions, world-leading industry best practices, and high-impact public awareness and education campaigns.

The key to achieving practical results in the ongoing fight against spam will be in continuing to coordinate the actions of all stakeholders through good communications.

The Need for a Comprehensive Strategy to Fight Threats to the Internet

The third major lesson the Task Force has learned is that the fight against spam is only part of a much larger battle now beginning against emerging and potentially much more serious threats to the Internet as a platform for communications and commerce.

When Canada began developing *An Anti-Spam Action Plan* two or three years ago, spam was seen mainly as a time-wasting annoyance for consumers and businesses. This was still the general view of spam when the Task Force began its work.

During the past year, the Task Force has come to appreciate that spam is much more than a mere nuisance. Spam is increasingly associated with activities that are intended to mislead and deceive, to violate privacy, to make unauthorized use of consumer or business equipment, to cause harm to computers or networks, to commit fraud or to steal personal information.

During this same period, spam and these other kinds of threats have begun to spread from Internet email to instant messaging and wireless communication services.

In preparing our report, we have therefore tried to look beyond the familiar problem of unsolicited commercial email, and to take a comprehensive, strategic view of the challenges and opportunities facing Canada from spam and other threats to the Internet.

Recommendations

To combat spam, we recommend the following actions:

Leadership and partnership

1. The federal government, in partnership with other stakeholders should continue to pursue a multifaceted strategy for stopping spam.

Legislation, regulation and enforcement

2. The federal government should establish in law a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet (e.g. botnets, spyware, keylogging) by enacting new legislation and amending existing legislation as required.
3. To this end, the following email activities and practices should be made offences in spam-specific legislation (these provisions may also be reflected, in whole or in part, in existing legislation):
   - the failure to abide by an opt-in regime for sending unsolicited commercial email;
   - the use of false or misleading headers or subject lines (i.e. false transmission information) designed to disguise the origins, purpose or contents of an email, whether the objective is to mislead recipients or to evade technological filters;
   - the construction of false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit other offences listed);
   - the harvesting of email addresses without consent, as well as the supply, use or acquisition of such lists; and
   - dictionary attacks.

4. For these new offences, the following penalties and remedies should be applicable:

   - The new offences created should be civil- and strict-liability offences, with criminal liability open for more egregious or repeated offences. There should be meaningful statutory penalties for all offences listed in Recommendation #3.

   - There should be an appropriate private right of action available to persons, both individuals and corporations. There should be meaningful statutory damages available to persons who bring civil action.

   - The businesses whose products or services are being promoted by way of spam should also be held responsible for the spamming. Responsibility should also rest with other third-party beneficiaries of spam.

5. Regarding the enforcement and administration of new legislation:

   - the administration of a new stand-alone law should be undertaken by the Minister of Industry, with support from a separate body responsible for policy oversight and coordination, public education and awareness, and support to enforcement agencies; and

   - enforcement of legislative provisions addressing spam should be undertaken by existing agencies.

6. The federal government should place priority on anti-spam enforcement by providing stronger support and dedicated resources to agencies to administer and enforce new and existing anti-spam legislation.

7. The federal government, in coordination with the provinces and territories, should conclude and implement cooperative enforcement agreements with other countries. These efforts should include examining and amending existing legislative provisions as required to allow for seamless international cooperative investigation and enforcement action.

Best practices for Internet service providers and other network operators

8. ISPs and other network operators should implement the best practices recommended by the Task Force on Spam.

9. ISPs and other network operators, in cooperation with the coordination body established by the Minister of Industry (pursuant to Recommendation 5) should, on an ongoing basis, measure the scope of the spam problem in Canada and assess the impact of the recommended practices. They should continue to identify issues that may require further study, with a view to developing additional recommendations.

10. To assist in the ongoing monitoring of spam trends and the continued development of anti-spam measures and techniques, the federal government should lead in establishing a Canadian spam database (i.e. the "Spam Freezer").

11. ISPs and other network operators should adopt and enforce Acceptable Use Policies (AUPs) that clearly prohibit spamming activities on their networks.

Best practices for email marketing

12. Commercial email marketers should implement the best business practices recommended by the Task Force on Spam and should, in cooperation with the coordination body established by the Minister of Industry, monitor the effectiveness of these practices on an ongoing basis.

13. Canadian industry, in coordination with international standards-development organizations, should continue to investigate various certification methodologies and their associated costs to determine which, if any, would provide the most suitable certification regime for Canada.

14. To help determine the extent of the problem of non-deliverability of legitimate email in Canada, the coordination body established by the Minister of Industry should, with the help of appropriate stakeholders, formally study this issue on an ongoing basis.

User awareness and education

15. As part of its ongoing effort to increase user awareness and education, the federal government, in cooperation with interested stakeholders, should continue to promote the "Stop Spam Here / Arrêtez le pourriel ici" user-tips campaign by encouraging others to link to these websites, and through the use of other appropriate methods and media.

16. The federal government, in cooperation with interested stakeholders, should continue to maintain and enhance the "Stop Spam Here / Arrêtez le pourriel ici" websites in order to increase their value as education tools and sources of appropriate links to other anti-spam resources, and so as to ensure that they remain up to date and relevant (e.g. by including information on industry best practices and future anti-spam legislation and complaints procedures).

17. The federal government, in cooperation with interested stakeholders, should develop appropriate and consistent anti-spam education and awareness campaigns tailored to the needs of different target audiences.

International cooperation

18. The federal government should continue to pursue bilateral agreements on anti-spam policies and strategies with foreign governments.

19. The federal government, in consultation, collaboration and partnership with other stakeholders as appropriate, should actively promote and assist the coordinated international implementation of anti-spam policies, laws, regulations and enforcement measures; industry standards and practices; and public education and awareness activities.

20. Canada should make its expertise in developing multistakeholder toolkit approaches to combatting spam available to help developing countries.

Establishment of a coordinating body

21. In order to carry forward the multifaceted, multistakeholder approach that has been developed by the Task Force on Spam, and to provide a focal point for facilitating the implementation of its recommendations, the federal government should establish a centre, reporting to the Minister of Industry, responsible for policy oversight and coordination, public education and awareness, and providing support to enforcement agencies.

22. The federal government, through this coordinating body, should monitor the impact of the implementation of the Task Force's recommendations; evaluate the results; provide regular public reports; and, in consultation with stakeholders, take whatever additional measures are necessary to combat spam.

1 DRAWING THE LINE

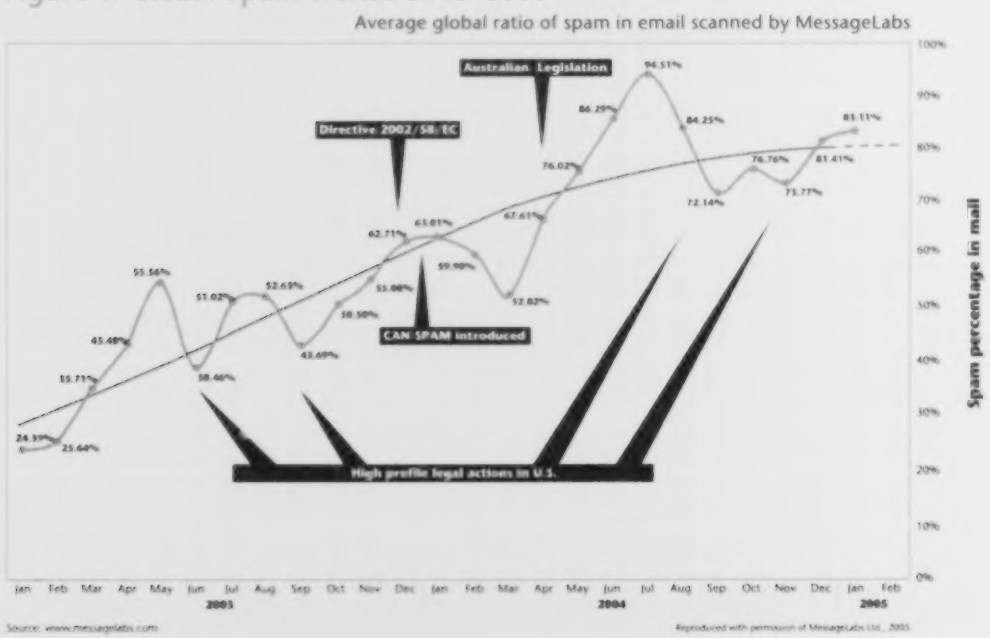
WHAT IS SPAM AND WHY IS IT A PROBLEM?

In just a few years, unsolicited commercial email, now generally known as "spam," has gone from being a minor nuisance to becoming a significant social and economic issue, a drain on the business and personal productivity of Canadians, and a cloak for criminal activity. Spam impedes the efficient use of the Internet for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce.

In 2000, email traffic reports indicated that spam amounted to about 10 percent of the total volume of electronic mail. As the chart presented in Figure 1 shows:

- by the end of 2002, the amount of spam had climbed to 30 percent;
- by the middle of 2003, the amount of unsolicited commercial email had surpassed that of legitimate communications; and
- by the end of 2004, spam made up 80 percent of global email.

Figure 1: Global Spam Trends 2003–2005



Source: www.messagelabs.com

Reproduced with permission of MessageLabs Ltd., 2005

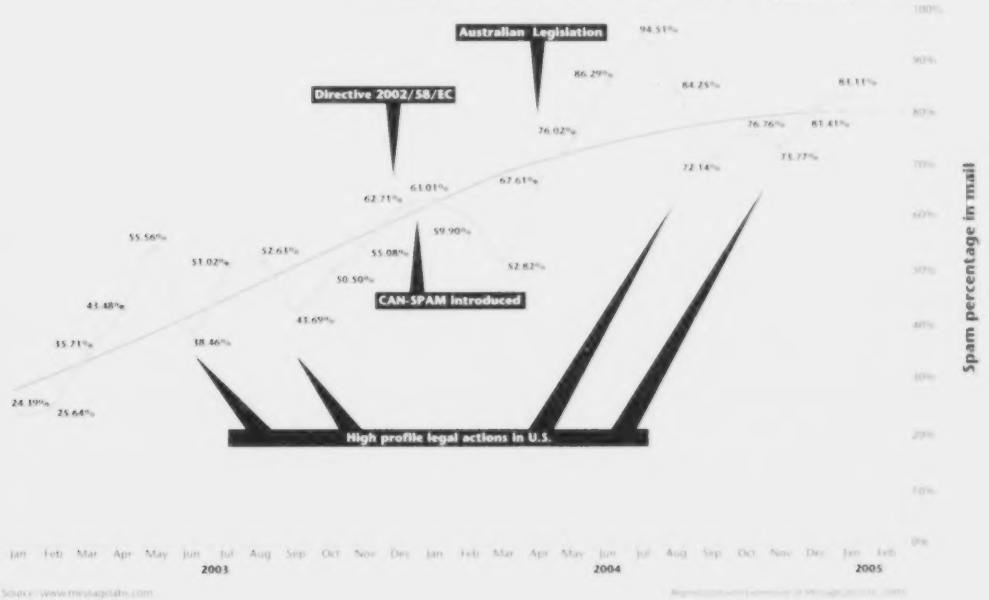
1 DRAWING THE LINE

In just a few years, unsolicited commercial email, now generally known as "spam," has gone from being a minor nuisance to becoming a significant social and economic issue, a drain on the business and personal productivity of Canadians, and a cloak for criminal activity. Spam impedes the efficient use of the Internet for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce.

In 2000, email traffic reports indicated that spam amounted to about 10 percent of the total volume of electronic mail. As the chart presented in Figure 1 shows:

- by the end of 2002, the amount of spam had climbed to 30 percent;
- by the middle of 2003, the amount of unsolicited commercial email had surpassed that of legitimate communications; and
- by the end of 2004, spam made up 80 percent of global email.

Average global ratio of spam in email scanned by MessageLabs



Source: www.messagelabs.com

The growing volume of spam is now a well-recognized pricing factor for companies that provide facilities for Internet services. This cost is ultimately paid for by organizations and businesses that use electronic communications to conduct their business. It is also paid for by personal users who communicate through the Internet with family, friends and others.

While the overall volume of spam continues to rise, the nature of the spam threat continues to evolve. Improved filtering techniques and other anti-spam safeguards adopted by ISPs and consumers have helped to somewhat reduce the number of spam messages that are reaching the mailboxes of individual Internet users. One public opinion survey, published in Ipsos-Reid's *Canadian Inter@ctive Reid Report* for the fourth quarter of 2004, reported that Canadians believe they are receiving less spam now than a year ago. Nevertheless, as Figure 1 illustrates, the persistent upward trend remains a significant problem for ISPs and users because of the costs of blocking or removing spam from networks.

More significantly, there is disturbing evidence that, even if the volume of traditional spam were to decline, the incidence of new threats posed by mutations of spam would still clearly be on the rise. These broader threats to Internet security include spyware, viruses, phishing and botnets, to name but a few. Recent reports show that these threats have dramatically increased in the year since the Task Force began its work. For example:

- MessageLabs reported seeing 18 million phishing emails in 2004.
- The October 2004 AOL®–National Cyber Security Alliance *Online Safety Study* reported that 80 percent of American users have spyware or adware on their computers, and that 89 percent of those users did not know that these programs were there.

The new mutations of spam undermine consumer confidence in the Internet as a platform for commerce and communications. Because of this, the potential of information and communications technology to buttress productivity, and the ability of e-commerce to attract investment, create jobs and enrich our lives, is constrained not only by torrents of spam, but by the deceptive, fraudulent and malicious activities that sometimes accompany it.

Principles Guiding Canada's Anti-Spam Action Plan

The degree of public concern and the growing costs to our economy have made it clear that government, industry, marketers and consumers must work together in a new partnership to reduce and control spam.

It is also apparent that spam is a multifaceted problem that requires coordinated action on several fronts in order to achieve real and measurable progress. Canadian stakeholders and international partners are all in agreement on the following principles:

- Commercial email sent with the prior and ongoing consent of the recipient is not spam and has a legitimate place in e-commerce.
- Commercial email sent without prior consent — or that is deceptive, fraudulent or malicious — is spam and should be prohibited.
- There is merit in examining the use of current laws and possible new laws to fight spam. However, unless enforcement agencies assign a high priority and allocate sufficient resources to anti-spam actions, laws alone will not stop spam and related threats, even if these laws are accompanied by technical measures, better business practices and changes in consumer behaviour.
- There is a consensus that government should not dictate detailed technical solutions. Instead, government should encourage and assist all partners in using and sharing the best available technical solutions and the best consumer and business practices.

- An effective solution to spam will require not only concerted actions by all partners in Canada, but also greater cooperation at the international level. Although Canada, unfortunately, remains a source of some spam, the great majority of spam emails received by Canadians originate outside Canada. An effective international response to spam will require a coordinated international approach involving governments and other stakeholders.

Mandate, Structure and Working Methods of the Task Force on Spam

On May 11, 2004, the Minister of Industry announced *An Anti-Spam Action Plan for Canada* designed to reduce the volume of unsolicited commercial email, and established a Task Force on Spam to oversee the implementation of the Action Plan. Chaired by Industry Canada, the Task Force brought together experts and key stakeholders representing ISPs, Canadian businesses that use email to conduct legitimate commercial activities and consumers.

The Task Force was given one year to oversee and coordinate the implementation of the Action Plan. After this period, the Task Force was asked to report on the progress made and to propose any new actions that might be required, including legislative initiatives.

Despite its relatively small number of members, the Task Force represented a broad range of organizations with stakes in the future of email communications, from individual users to large companies that develop and supply the software and equipment that fuels Internet growth. In order to organize its work and engage other stakeholders, the Task Force established five working groups, under the following titles, to address specific points contained in the Action Plan:

- Legislation and Enforcement
- Network and Technology Management
- Validating Commercial Email
- Public Education and Awareness
- International Collaboration

Membership in the working groups was open to all interested individuals and organizations. About 60 organizations answered the call. These are listed in Appendix A.

During its mandate, the Task Force was asked to bring key stakeholders together to review the implementation of the Action Plan and identify any other areas that might require further action. This was done through a national Stakeholder Roundtable held December 3, 2004.

The Task Force was also asked to consult all interested stakeholders and individual Canadians who might wish to express their views or make a contribution to its work. To do this, the Task Force issued a notice in the *Canada Gazette* in summer 2004, and established an online forum where individuals could express their views on any of the subject areas under consideration by the Task Force.

General Recommendation

The Task Force's experience has shown the value and necessity of continuing with a multifaceted, multistakeholder approach to combatting spam. Although significant progress has been made in the fight against unsolicited commercial email during the past year, much remains to be done.

In addition, the new and much more serious threats to Internet security that are now emerging — such as spyware and identity theft resulting from phishing and other illegal online activities — heighten the importance of maintaining the multistakeholder momentum developed by the Task Force.

The Task Force has come to the conclusion that, in order to successfully wage the war against spam, it is necessary to establish a focal point that has the responsibility of coordinating the ongoing battle against spam and the illegal activities associated with it.

We therefore recommend the following:

Recommendation 1:

The federal government, in partnership with other stakeholders, should continue to pursue a multifaceted strategy for stopping spam.

2 CLARIFYING THE RULES

THE CHALLENGE

Traditional markets for physical goods and services operate in the context of laws and regulations designed to promote fair competition and protect consumers. To work effectively, e-commerce markets need similar rules to guide commercial behaviour. As discussed in the previous chapter, spam presents a significant threat to the development of e-commerce by imposing costs, creating inefficiencies, causing harm and undermining the confidence of business and consumers alike.

Some of the threats posed by spam can be dealt with by enforcing existing legislation, raising business and consumer awareness, and promoting public education. However, these measures are unlikely to succeed against the truly bad who are found among spammers — those whose intent is to commit fraud, steal personal identity, violate privacy, gain unauthorized access, or cause harm to computers and network equipment. Clearer laws prohibiting illegitimate behaviour, strong penalties and rigorous enforcement are needed to deal with these kinds of threats, and to underpin Canada's toolkit approach to fighting spam.

A strong domestic framework will become even more crucial as spam increasingly becomes the vehicle for activities such as phishing, and technology such as spyware, viruses and botnets, which pose a serious threat to the Internet as an economic platform by undermining trust. The Internet has become part of our nation's critical infrastructure and we must, as a country, be able to effectively address these threats to its security.

A strong domestic framework is also needed if we are going to play our part in fighting spam worldwide. The vast majority of spam reaching Canadian citizens and businesses originates outside Canada. However, with a clear, solid legislative framework in place, and with effective enforcement capabilities and efforts, Canada would be well positioned to work towards internationally harmonized approaches and cooperative enforcement actions.

One of the first questions facing the Task Force on Spam was how well Canada's current legal and enforcement framework measured up to the challenge of combatting spam.

When *An Anti-Spam Action Plan for Canada* was being developed, many stakeholders expressed the view that improving the enforcement of existing Canadian laws could significantly reduce the flow of spam. Specifically, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the *Competition Act* and the *Criminal Code* of Canada were cited, on the following grounds, as tools that could help address the problem of unsolicited email.

- PIPEDA, designed to protect personal information in the electronic age, prohibits the collection, use or disclosure of personal information, including email addresses, without consent. This law also specifies that personal information can only be used for the purpose for which it was collected, and that consent is required for any further secondary use. Thus, any unsolicited email sent to the email

address of an individual who did not consent to receive that email could be in violation of this federal Act and, possibly, other substantially similar provincial legislation.

- The *Competition Act* contains provisions dealing with deceptive and misleading representations. These have frequently been used to deal with misleading advertising in traditional media. The application of this Act to misleading claims made in email solicitations clearly merited examination.
- The *Criminal Code* of Canada contains specific provisions dealing with unauthorized access to computer systems and networks, mischief to data and more general fraud provisions. Since many email abusers send "Trojan" programs embedded in email messages, which can then be activated by spammers to relay spam, the *Criminal Code* could possibly be used to address these spam-related offences. Its provisions include substantial fines and even imprisonment.

Although these existing acts were identified as having provisions that could potentially be used in the fight against spam, the Task Force noted that their effectiveness remained an open question, since most had not yet been used in spam-related cases.

The first challenge facing the Task Force, therefore, was to determine the adequacy of Canada's current legal and enforcement framework in the fight against spam. To respond to this challenge, the Task Force decided to work with other government departments and agencies to examine existing laws and enforcement mechanisms to see if there were any gaps that could prevent them from being useful parts of the anti-spam toolkit.

Since this proved to be the case, the second challenge facing the Task Force was to determine what measures would be required to fill these gaps, so that Canada would have an effective legal framework and a coordinated, national enforcement approach for dealing with spam and related activities.

Task Force Actions

Raising Awareness and Catalyzing Action by Enforcement Agencies

The Task Force initially focused on facilitating discussions among private companies and the federal enforcement agencies responsible for legislation that could be used to address spam. These agencies included the Competition Bureau, the Office of the Privacy Commissioner of Canada and the RCMP (Royal Canadian Mounted Police). The intention was to evaluate how effective the individual statutes would be in prosecuting offences related to spam.

First, all federal statutes that could apply to elements of spam were identified. The Task Force decided to focus its efforts on those elements of spam that had the clearest links to provisions in existing statutes. A number of smaller task groups were established to discuss the requirements of different situations involved in pursuing cases under each statute. As of the release of this report, three complaints had been settled under PIPEDA, and one under the *Competition Act* (see Box 1: Recent Spam-Related Cases).

Little progress was made with respect to the *Criminal Code* of Canada, because of a lack of prioritization and jurisdiction, since primary responsibility for prosecution rests with provincial governments and local law enforcement agencies. However, the Task Force worked with these groups to advance the issue. In addition, the Task Force worked with the Department of Justice Canada and the RCMP's Technological Crime Branch to identify the general evidentiary requirements that would be involved in bringing cases forward under specific provisions of the *Criminal Code*.

Following discussions with the Canadian wireless communications industry, the possibility was raised of applying existing provisions of the *Telecommunications Act* to spam sent to wireless handsets. The passage of Bill C-37 (for the creation of a national do-not-call list) may provide an opportunity to strengthen the Canadian Radio-television and Telecommunications Commission's (CRTC's) ability to address wireless

Box 1: Recent Spam-Related Cases

Complaint Findings by the Office of the Privacy Commissioner of Canada
Two members of the Task Force on Spam filed complaints under PIPEDA.

Michael Geist received two email solicitations to purchase season tickets from a community football team. The team's office had obtained Geist's email address from university and law firm websites. He filed a complaint with the Privacy Commissioner after he received the second email, which was sent after Geist requested that he not receive further emails.

The Office of the Privacy Commissioner found that a business email address is personal information and, therefore, protected by PIPEDA. Such information can be collected and used without consent, but only for its intended purposes (i.e. purposes related to Geist's business as professor and lawyer). The Commissioner concluded that the football team could not rely on this exception, since its purposes were entirely unrelated to the intentions of publishing the email address.

Suzanne Morin received email solicitations, from a different company than Geist, at her business email address. Her email address was collected from an online professional association membership directory. She filed a complaint with the Privacy Commissioner. The Office of the Privacy Commissioner again found that a business email address is, for the purposes of PIPEDA, personal information. The Office found that the collection and subsequent use of Morin's email address for commercial email solicitation were done by the marketing company without her consent, in contravention of the Act.

In both cases, the organizations apologized for their actions, removed the email addresses from their email marketing lists and amended their internal practices accordingly.

Resolution of a Case by the Competition Bureau
Performance Marketing Ltd. made false claims about Zyapex and Dyapex Diet Patches, promoting them as safe and natural weight-loss products, giving the impression that without performing any physical exercise or dieting a person could lose weight, reduce their appetite, control their cravings and speed up their metabolism. These claims were made via email. Performance Marketing Ltd. failed to enforce its anti-spam policy, which led to its affiliates using spam to sell the products.

The case was pursued under the Competition Bureau's Project FairWeb, which is aimed at combatting misleading and deceptive advertising on the Internet. According to the resulting Consent Agreement with Performance Marketing issued in December 2004, the company has agreed to ensure that spam will not be used as a vehicle for marketing its products, to post a corrective notice on its website and to provide a full refund to those who purchased the diet patches.

spam — specifically, emailing of SMS (Short Message Service) spam to mobile handsets. Of particular importance would be the CRTC's fining authority. Until Bill C-37 is passed, it may be too early to judge the role that the *Telecommunications Act* could play.

The Problem of Enforcement

The initial stages of the Task Force on Spam's work served to educate both enforcement agencies on the extent and severity of the spam problem; and private companies on the legal requirements, including evidentiary requirements, for the successful pursuit of cases. Parallel with this work, some enforcement agencies have taken direct action against spammers (see Box 1 above). Nevertheless, the overall effectiveness of enforcement efforts to date has been limited.

The enforcement agencies face a number of challenges related to the use of their legislation to address all the various elements of the spam problem. Limited resources and competing priorities are significant factors hindering the two regulatory bodies involved, as well as the RCMP and local law enforcement agencies. A further impediment to effective enforcement is the frequent lack of specialized technical expertise needed to track down, investigate and prosecute spammers. Finally, in many cases, existing enforcement powers have not yet been used, and the legislative tools to attack particular elements of spam are either too uncertain in their application or simply missing.

The Task Force strongly believes in the need to strengthen the enforcement process. This should begin with a clear policy commitment to curbing spamming and spam-like activities by not only responding to complaints but also proactively investigating and prosecuting spammers.

Box 1: Recent Spam-Related Cases

Complaint Findings by the Office of the Privacy Commissioner of Canada
Two members of the Task Force on Spam filed complaints under PIPEDA.

Michael Geist received two email solicitations to purchase season tickets from a community football team. The team's office had obtained Geist's email address from university and law firm websites. He filed a complaint with the Privacy Commissioner after he received the second email, which was sent after Geist requested that he not receive further emails.

The Office of the Privacy Commissioner found that a business email address is personal information and, therefore, protected by PIPEDA. Such information can be collected and used without consent, but only for its intended purposes (i.e. purposes related to Geist's business as professor and lawyer). The Commissioner concluded that the football team could not rely on this exception, since its purposes were entirely unrelated to the intentions of publishing the email address.

Suzanne Morin received email solicitations, from a different company than Geist, at her business email address. Her email address was collected from an online professional association membership directory. She filed a complaint with the Privacy Commissioner. The Office of the Privacy Commissioner again found that a business email address is, for the purposes of PIPEDA, personal information. The Office found that the collection and subsequent use of Morin's email address for commercial email solicitation were done by the marketing company without her consent, in contravention of the Act.

In both cases, the organizations apologized for their actions, removed the email addresses from their email marketing lists and amended their internal practices accordingly.

Resolution of a Case by the Competition Bureau
Performance Marketing Ltd. made false claims about Zyapex and Dyapex Diet Patches, promoting them as safe and natural weight-loss products, giving the impression that without performing any physical exercise or dieting a person could lose weight, reduce their appetite, control their cravings and speed up their metabolism. These claims were made via email. Performance Marketing Ltd. failed to enforce its anti-spam policy, which led to its affiliates using spam to sell the products.

The case was pursued under the Competition Bureau's Project FairWeb, which is aimed at combatting misleading and deceptive advertising on the Internet. According to the resulting Consent Agreement with Performance Marketing issued in December 2004, the company has agreed to ensure that spam will not be used as a vehicle for marketing its products, to post a corrective notice on its website and to provide a full refund to those who purchased the diet patches.

spam — specifically, emailing of SMS (Short Message Service) spam to mobile handsets. Of particular importance would be the CRTC's fining authority. Until Bill C-37 is passed, it may be too early to judge the role that the *Telecommunications Act* could play.

The Problem of Enforcement

The initial stages of the Task Force on Spam's work served to educate both enforcement agencies on the extent and severity of the spam problem; and private companies on the legal requirements, including evidentiary requirements, for the successful pursuit of cases. Parallel with this work, some enforcement agencies have taken direct action against spammers (see Box 1 above). Nevertheless, the overall effectiveness of enforcement efforts to date has been limited.

The enforcement agencies face a number of challenges related to the use of their legislation to address all the various elements of the spam problem. Limited resources and competing priorities are significant factors hindering the two regulatory bodies involved, as well as the RCMP and local law enforcement agencies. A further impediment to effective enforcement is the frequent lack of specialized technical expertise needed to track down, investigate and prosecute spammers. Finally, in many cases, existing enforcement powers have not yet been used, and the legislative tools to attack particular elements of spam are either too uncertain in their application or simply missing.

The Task Force strongly believes in the need to strengthen the enforcement process. This should begin with a clear policy commitment to curbing spamming and spam-like activities by not only responding to complaints but also proactively investigating and prosecuting spammers.

While increasing resources, both in the form of funding and technical expertise, is essential, increased support for enforcement agencies should also take the form of better mechanisms for collecting, coordinating and processing information on spam, including that which is received from user complaints. Chapter 7 of this report discusses these mechanisms. Last, but not least, we must fill the gaps that exist in the legal and regulatory regime governing spam and other threats to the Internet, such as spyware.

Legal Research

As background to its deliberations, the Task Force researched spam legislation in other countries, with a particular focus on the United States, the United Kingdom and Australia, in order to benchmark Canada's current situation in relation to these jurisdictions. Box 2: International Anti-Spam Legislation highlights the legislation in place in a number of key countries.

The Task Force also commissioned a study examining the issue of a private right of action for spam in Canada, including the existing legislative framework, the key elements of building such a right and the views of Canadian companies on the need for such a right.

Identification of Legislative Gaps

After reviewing existing legislation and enforcement activities, taking into account the experience of other countries that have already enacted broad-based anti-spam laws, and reviewing the results of the cases triggered by the Task Force and the resulting lessons learned, a number of gaps in existing Canadian legislation and enforcement became evident.

The existing provisions of the three relevant acts, while applicable to some elements of spamming activity, could not be used with sufficient certainty to effectively address many of the methods and means used by spammers. Nor could they be used against some of the more aggressive and invasive forms of spamming, or to counter the new threats to Internet security that are emerging. Agencies are limited in their enforcement powers by the scopes and purposes of their acts, and, as the laws are currently written, many spamming and spam-related activities fall outside these boundaries.

Box 2: International Anti-Spam Legislation

United States — *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CAN-SPAM Act of 2003)

Australia — *Spam Act 2003*

United Kingdom — *Privacy and Electronic Communications Regulations 2003*

France — *Loi pour la confiance dans l'économie numérique 2004*

European Union — EC Directive 2003/58/EC

An additional gap was identified related to deterrence. Where the acts did apply, the question remained "Are the penalties appropriate to deter spamming activities?" The Task Force determined that, while existing mechanisms may be adequate when used against legitimate companies who have spammed in error, it is not clear whether they would deter truly bad actors. Even when significant penalties are available, as through the *Criminal Code*, the practicality of applying them in spam-related cases is limited.

A Framework for Spam Legislation and Enforcement

After fully assessing the adequacy of existing legislation and enforcement capabilities in light of the threats posed by spam and spam-related activities, the Task Force came to the following conclusions:

- While existing laws address specific aspects of spam, they are not, separately or together, sufficient to achieve the overall goal of deterring spammers in Canada.
- A stand-alone, technology-neutral law that clearly addresses spam, spam-related offences and emerging threats (e.g. botnets, spyware and keylogging) is required. Amendments to existing laws may also be required.

Nature of Offences and Remedies/Penalties

- Failure to abide by an opt-in regime for sending unsolicited commercial email should be made an offence in a stand-alone, technology-neutral spam statute.
- The use of false or misleading headers or subject lines (i.e. false transmission information) designed to disguise the origins, purpose or contents of an email should be made an offence. This should be the case whether the objective is to mislead recipients or to evade technological filters.
- Constructing false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit the other offences listed) should be made an offence.
- The harvesting of email addresses without consent, and the supply, use or acquisition of such lists should be made an offence.
- Dictionary attacks should be made offences.
- The new offences created should be civil- and strict-liability offences, with criminal liability open for more egregious or repeated offences. There should be meaningful statutory penalties for all offences outlined above.
- There should be an appropriate private right of action available to persons, both individuals and corporations. There should be meaningful statutory damages available to persons who bring civil action.
- The businesses whose products or services are being promoted by way of spam should also be held responsible for the spamming. Responsibility should also rest with other third-party beneficiaries of spam.

Administration and Enforcement

- The Minister of Industry should be responsible for administering new legislation on spam, and a centre of responsibility should be established for policy oversight and coordination, public education and awareness, and support to enforcement agencies.
- Enforcement of new legislative provisions addressing spam should be undertaken by existing agencies.
- New and existing spam provisions must be accompanied by increases in dedicated resources and support for the agencies that will enforce them.
- Given that spam is a borderless problem, there is a need for provisions allowing for cooperative international enforcement and investigation. Any current provisions should be examined and amended as required to allow for seamless action on spam.

Regulatory Arrangements

Although the main focus of discussions among working group members was the prohibition of spamming and spam-related activities, there was some discussion at the Stakeholder Roundtable meeting in December 2004, as well as among Task Force members, about broader regulatory arrangements. Some argued for a "co-regulatory" approach, based on the Australian model, that would outline responsibilities, primarily for ISPs, in areas such as protecting networks against spam. Others maintained that the Canadian practice of voluntary cooperation and industry peer pressure would prove to be a faster and more effective way of fighting spam than the co-regulatory approach. While there was much debate on this topic, there was general agreement that government should play no role in dictating specific technical solutions, and that the legislative ground rules (including those outlined above) should be technology-neutral.

Although industry efforts to address the problem of spam were already under way, the experience of the Task Force has demonstrated the value of government–industry dialogue in catalyzing private sector action. The Task Force, therefore, considers continued government–industry dialogue in this area essential. The Task Force has also noted that broader questions about Internet regulation should be addressed through the Telecommunications Policy Review announced by the Government of Canada in the federal Budget 2005.

Recommendations

It is clear to the Task Force, from our analysis of the Canadian situation and the experiences of other countries, that Canada will not be able to combat spam effectively within Canada unless its multistakeholder toolkit approach includes a clearer, more comprehensive, and actively enforced set of domestic laws that protect Internet users and facilitate the development of e-commerce.

We therefore recommend the following:

Recommendation 2:

The federal government should establish in law a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet (e.g. botnets, spyware, keylogging) by enacting new legislation and amending existing legislation as required.

Recommendation 3:

To this end, the following email activities and practices should be made offences in spam-specific legislation (these provisions may also be reflected, in whole or in part, in existing legislation):

- **the failure to abide by an opt-in regime for sending unsolicited commercial email;**
- **the construction of false or misleading headers or subject lines (i.e. false transmission information) designed to disguise the origins, purpose or contents of an email, whether the objective is to mislead recipients or to evade technological filters;**
- **constructing false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit other offences listed);**
- **the harvesting of email addresses without consent, as well as the supply, use or acquisition of such lists; and**
- **dictionary attacks.**

Recommendation 4:

For these new offences, the following penalties and remedies should be applicable:

- **The new offences created should be civil- and strict-liability offences, with criminal liability open for more egregious or repeated offences. There should be meaningful statutory penalties for all offences listed in Recommendation #3.**
- **There should be an appropriate private right of action available to persons, both individuals and corporations. There should be meaningful statutory damages available to persons who bring civil action.**
- **The businesses whose products or services are being promoted by way of spam should also be held responsible for the spamming. Responsibility should also rest with other third-party beneficiaries of spam.**

Recommendation 5:

Regarding the enforcement and administration of new legislation:

- **the administration of a new stand-alone law should be undertaken by the Minister of Industry, with support from a separate body responsible for policy oversight and coordination, public education and awareness, and support to enforcement agencies; and**
- **enforcement of legislative provisions addressing spam should be undertaken by existing agencies.**

Recommendation 6:

The federal government should place priority on anti-spam enforcement by providing stronger support and dedicated resources to agencies to administer and enforce new and existing anti-spam legislation.

Recommendation 7:

The federal government, in coordination with the provinces and territories, should conclude and implement cooperative enforcement agreements with other countries. These efforts should include examining and amending existing legislative provisions as required to allow for seamless international cooperative investigation and enforcement action.

3 MANAGING NETWORKS TO STOP SPAM

THE CHALLENGE

Any measure aimed at successfully protecting the security of Internet communications from threats such as spam, viruses and spyware must involve more than government actions. There is consensus among stakeholders on a number of steps that can be taken by ISPs and other network operators (e.g. large enterprise users, universities, government departments) to build trust in Internet communications.

Some of these initiatives relate to the development and application of technology. Others relate to the implementation of best practices within the industry, including Acceptable Use Policies that prohibit spamming. All of these industry initiatives are based on a common goal: ensuring that email remains a viable tool for legitimate business and personal communications.

By its design and architecture, the Internet is an open network of networks that allows the free flow of information. The redesign and implementation of technical standards to enhance security and curtail abuse will be ongoing over many years.

There are, however, a number of known practices that permit spam and other forms of network abuse to happen. These include leaving servers open to relay and forward messages, thereby allowing computer systems to be hijacked as proxy email servers for abusers. Some steps have been taken by several organizations to warn businesses and network managers about the importance of securing systems and networks, but adoption of these practices remains uneven.

While the problem of spam, like itself, is global in scope, network- .nt actions taken in Canada can contribute to the solution. Those who own and manage networks and facilities must address and adopt management practices that will effectively reduce and control spam and related threats.

Canadian industry stakeholders have the ability to agree on basic operating practices for network facilities that will reduce spam, and can show leadership by requiring the adoption of these practices on networks and facilities based in Canada.

Task Force Actions

The Task Force on Spam represents the first-ever collaborative, concerted effort involving a broad range of organizations, including most of the country's largest and smallest broadband and dial-up ISPs, other network operators, large enterprise users, software developers, anti-spam advocates and government. The agreement by these stakeholders to work together to develop and implement industry-wide spam solutions is an important step forward. However, it is only the beginning of a long-term commitment to taking the actions necessary to stop spam.

Box 3: Recommended Best Practices for Internet Service Providers and Other Network Operators

- All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.
- ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive email over port 25 should be restricted to hosts and the provider's network. Use of port 25 by end-users should be permitted only on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.
- ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.
- ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.
- ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.
- ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.
- ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.
- ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).
- Non-delivery notices (NDNs) should only be sent for legitimate emails.
- ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.
- ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFC) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.
- ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822; and reference domains and IP addresses should have up-to-date, accurate registration information.

Recommended Best Practices for Internet Service Providers and Other Network Operators

The Task Force has developed a set of recommended technical best practices intended to help reduce spam in Canada. Box 3 above presents the highlights of that document. The adoption of these practices will also address spam-related security issues, since spam is often the vehicle for more harmful activities. The practices represent a continuation of efforts and progress that have been under way for some time in Canada and internationally. The Task Force has advanced this work to establish the first truly national consensus on recommended technical measures for combatting spam. Through these best practices, Canada has a model to share internationally in the global fight against spam. However, it will be important to continually update these best practices to reflect the continuing evolution of spam trends and techniques.

The full text of the best practices recommended by the Task Force is presented in Appendix B.

Measuring Implementation and Impact

A substantial number of Canadian ISPs, including many of the major players and other network operators, have started to implement some or all of the recommended technical practices, particularly by blocking port 25 and upgrading their filtering techniques.

The experiences of other countries have shown that ISPs themselves, particularly market leaders, can do much to spread the adoption of anti-spam technical and business best practices throughout the industry. The leadership already shown by some Canadian ISPs in implementing the recommended best practices has been instrumental in encouraging other ISPs to do likewise.

Box 3: Recommended Best Practices for Internet Service Providers and Other Network Operators

- All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.
- ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive email over port 25 should be restricted to hosts and the provider's network. Use of port 25 by end-users should be permitted only on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.
- ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.
- ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.
- ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.
- ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.
- ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.
- ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).
- Non-delivery notices (NDNs) should only be sent for legitimate emails.
- ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.
- ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFC) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.
- ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822; and reference domains and IP addresses should have up-to-date, accurate registration information.

Recommended Best Practices for Internet Service Providers and Other Network Operators

The Task Force has developed a set of recommended technical best practices intended to help reduce spam in Canada. Box 3 above presents the highlights of that document. The adoption of these practices will also address spam-related security issues, since spam is often the vehicle for more harmful activities. The practices represent a continuation of efforts and progress that have been under way for some time in Canada and internationally. The Task Force has advanced this work to establish the first truly national consensus on recommended technical measures for combatting spam. Through these best practices, Canada has a model to share internationally in the global fight against spam. However, it will be important to continually update these best practices to reflect the continuing evolution of spam trends and techniques.

The full text of the best practices recommended by the Task Force is presented in Appendix B.

Measuring Implementation and Impact

A substantial number of Canadian ISPs, including many of the major players and other network operators, have started to implement some or all of the recommended technical practices, particularly by blocking port 25 and upgrading their filtering techniques.

The experiences of other countries have shown that ISPs themselves, particularly market leaders, can do much to spread the adoption of anti-spam technical and business best practices throughout the industry. The leadership already shown by some Canadian ISPs in implementing the recommended best practices has been instrumental in encouraging other ISPs to do likewise.

While this is an encouraging beginning, it will clearly be necessary to systematically monitor the implementation of the recommended best practices, in order to assess their impact and identify any new problems that may need to be addressed through amendments or additions to the best-practices provisions. If this is not done, it will be difficult for industry, government policy-makers and other stakeholders to determine the level to which industry has adopted the recommended best practices, or to measure their effectiveness in the fight against spam.

In the spirit of industry self-regulation, the Task Force encourages the major players in the ISP and network-operator communities to continue to show leadership in implementing the recommended best practices, and to encourage others to follow their example.

The Task Force also calls on the major players and relevant industry associations to play an active role, together with the coordination body described in Chapter 7, in helping develop an effective system for measuring and publicly reporting on the impact of the recommended best practices.

Canadian Spam Database ("Spam Freezer")

The Task Force on Spam evaluated the idea of establishing, under a public–private sector partnership, a Canadian spam database, or "Spam Freezer," similar in design to the "Spam Fridge" maintained and monitored by the U.S. Federal Trade Commission (FTC).

The objective of a Canadian database would be to provide a repository to which email users could send copies of spam received in their computer mailboxes. Spam messages sent to the database would be inventoried and kept for a prescribed period of time by a Canadian organization with central coordinating responsibility in the fight against spam.

The database would provide an opportunity for law enforcement agencies from Canada and possibly other countries, ISPs, other network operators and various levels of government to access data that could be used for statistical analysis and to gather evidence for anti-spam enforcement activities.

Internet Email Spam Over Wireless Devices

Unlike the Internet, which developed as an open, public network, mobile technologies were originally deployed on closed, private networks.

Convergence of technologies and increased interaction between the Internet and mobile technologies, however, mean that some of the problems that originally affected the Internet are beginning to affect mobile networks. This can happen when people use wireless devices to retrieve email, including spam, from their ISPs. It can also happen when people begin to receive new forms of spam originated on wireless networks and transmitted through mobile-phone text messaging (i.e. SMS), multimedia messaging and instant messaging services. These kinds of messaging services have become successful applications of mobile technology. They provide a host of possibilities for developing innovative services, but also give spammers new opportunities.

"Mobile" or "wireless" spam is potentially more problematic than spam sent to desktop computers, since wireless spam follows the customer and since, in some cases, customers pay a fee per message received. Wireless spam is a major annoyance to wireless subscribers, and can potentially be much more intrusive than spam sent to a personal computer.

The Task Force consulted with the Canadian wireless industry to discuss this issue and explore what might be done to prevent spam from becoming a major problem on wireless networks. Through these discussions, the Task Force learned that spam originating on wireless networks is perceived as a serious threat by wireless-network operators. The wireless industry is implementing

technical measures to protect its customers from wireless spam, and is also considering legal and regulatory remedies that could help prevent wireless spam.

Both the Task Force and wireless-industry representatives recognized that the anti-spam solutions adopted by the federal government and other stakeholders as a result of the Task Force's work and recommendations should be technology neutral, and applied to the wireless industry through the appropriate mechanisms.

Sharing Technical Information Among Internet Service Providers and Other Network Operators

Although industry has done a lot of good work to fight spam, and has reported some significant improvements as a result of these efforts, much remains to be done in terms of collaboration.

Key to success will be ISPs and other network operators' continued improvement of the sharing of spam-related information. To succeed in the fight against spam, it will be very important for ISPs and other network operators to deal with issues in a concerted way by communicating quickly and effectively on issues and problems of common concern, and by establishing appropriate intercompany processes to respond to incident reports.

Recommendations

ISPs and other network operators are on the front lines in the fight against spam. As the point of contact between those who originate spam and those who receive it, they are uniquely positioned to fight spam.

We therefore recommend the following:

Recommendation 8:

ISPs and other network operators should implement the best practices recommended by the Task Force on Spam.

Recommendation 9:

ISPs and other network operators, in cooperation with the coordination body established by the Minister of Industry (pursuant to Recommendation 5), should, on an ongoing basis, measure the scope of the spam problem in Canada and assess the impact of the recommended practices. They should continue to identify issues that may require further study, with a view to developing additional recommendations.

Recommendation 10:

To assist in the ongoing monitoring of spam trends and the continued development of anti-spam measures and techniques, the federal government should lead in establishing a Canadian spam database (i.e. the "Spam Freezer").

Recommendation 11:

ISPs and other network operators should adopt and enforce Acceptable Use Policies (AUPs) that clearly prohibit spamming activities on their networks.

4 RESTORING CONFIDENCE IN EMAIL

THE CHALLENGE

Before the establishment of the Task Force on Spam, most Canadian initiatives aimed at controlling the growing volume of unsolicited commercial email focused on a combination of filtering technologies and the use of "black lists" of servers and domains that have been identified as sources of spam. As these spam-control services have become more and more sophisticated, so have the tactics used by spammers to bypass them.

The diverse types of spam-filtering and blocking tools used by ISPs and other network operators — and the resulting cyclical battles between spammers and spam blockers — produced some unwanted results. Legitimate commercial email communications, as well as legitimate noncommercial and personal email communications, are now often blocked by filters, sometimes without the knowledge of either the senders or the intended recipients. These filtering techniques and practices, though well intended, have inadvertently contributed to undermining consumer confidence in the reliability of email.

For this reason, a number of commercial organizations are now considering moving their email services to closed networks, which would undermine the Internet as a platform for commerce. While the motivation for considering this solution is understandable, a migration of commercial activity away from the public Internet and toward closed networks could have undesirable consequences.

Less drastic alternatives to closed networks are beginning to emerge in the form of techniques that shift the focus away from blocking unwanted communications toward facilitating the movement of legitimate commercial email. Although these techniques impose costs on the senders of commercial email and on the owners and managers of network facilities, it is possible that these costs may be offset by the following benefits that could result for different stakeholders:

- for commercial email senders, the value of improved deliverability;
- for service providers, reduced costs in managing email service and customer preferences;
- for email users, more effective tools to manage their email.

Certification is one of the techniques emerging for improving deliverability. At minimum, a certification regime should require verifiable identification of both the sender and the nature of the communication. To be fully effective, it should also include performance-measurement tools and appropriate sanctions for certificate holders that do not abide by the rules.

In addition to certification tools, techniques are becoming available to facilitate the movement of legitimate email by authenticating sending and receiving sites. However, these techniques do not necessarily protect recipients against false, misleading or fraudulent emails sent from authentic sites.

Like the other parts of the anti-spam toolkit, established techniques, such as black lists and filtering, and emerging techniques, such as certification and authentication, are not silver bullets that will solve all deliverability problems. In addition to these technical solutions, there are a range of business practices that can be used by commercial emailers to reduce the incidence of spam and spam-related threats to the Internet. The overall challenge facing the commercial email business community is to identify and implement a winning combination of sound business practices and effective technical solutions.

Task Force Actions

The initial aim of the Task Force was to bring together, for the first time, a diverse group of stakeholders to discuss the challenges spam poses for legitimate emailers and address ways to improve the deliverability of legitimate email.

In addition to the technical tools described in the previous section, there are a number of business practices that can help combat spam and improve the deliverability of legitimate email. The Task Force, therefore, decided to devote a significant part of its efforts to the development of a code of best practices for emailers. The code would include both operational and technical measures that emailers could take to improve the deliverability of their messages.

The Task Force concluded that the Internet Engineering Task Force and its working groups were doing an effective job of managing and directing the development of authentication techniques. Therefore, we decided to concentrate our technical efforts on exploring email-certification techniques, raising awareness of their potential role in improving email deliverability and promoting discussion among industry segments.

Recommended Best Practices for Email Marketing

The code of recommended best practices for commercial emailers developed by the Task Force reflects the provisions of two policy frameworks — one legal and one self-regulatory — already in place in Canada:

- PIPEDA, which came into full force throughout Canada in January 2004, establishes the obligations of those who collect, store and use electronic-mail addresses, which are considered personal information.
- The Canadian Marketing Association has had a mandatory industry code for a number of years. Organizations that conduct online surveys (i.e. members of the Canadian Survey Research Council) are now also in the process of developing a uniform code of practice.

On this basis, and taking into account codes of practice that have been developed in other jurisdictions (e.g. by the U.S.-based Anti-Spam Technical Alliance), the Task Force finalized a series of recommended best practices that will encourage Canadian commercial emailers to adopt spam-free marketing and other spam-free business techniques, and make it clear that spam has no place in Canadian e-commerce.

The full text of these recommended best practices is presented in Appendix C. Box 4: Recommended Best Practices for Email Marketing presents the highlights of these best practices.

Deliverability of Commercial Email

There is currently significant evidence but a lack of statistics as to the extent to which legitimate commercial email is being blocked by spam-filtering programs and services — a process that creates what are known as "false positives" (i.e. blocked messages that are not really spam). A recent study by the firm Return Path determined that 22 percent of permission-based commercial email in the United States did not reach its intended recipients in 2004.

- Marketing email should only be sent to recipients who have provided their consent to receive such information.
- In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving all further business and/or marketing email messages from the organization.
- The internal process used to obtain consent should be clear and transparent. Organizations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.
- Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.
- Every email should provide a link to the sender's privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through "clickstream" means or other website monitoring techniques.
- Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.
- Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.
- When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.
- All email containing sexually explicit content should include the prefacing tag "SEXUALLY EXPLICIT" in the subject line.
- Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.
- Organizations may disclose the email addresses of existing customers to third-party affiliates or within a family of companies if:
  - they have consent to do so;
  - they are using the addresses for purposes consistent with their collection (i.e. marketing related to the original purchase or to provide services related to that purchase);
  - it is transparent to the recipient why they are receiving email communications; and
  - there is an easy-to-use way to opt out of receiving further email communications.

False positives are a problem, not only because they undermine the effectiveness of email as a marketing tool for businesses, but also because they cause difficulties for end-users, who are increasingly relying on the deliverability of the email they send and receive from associate sources, be they professional (e.g. business colleagues), commercial (e.g. as a result of marketing and online purchases the user has requested) or personal (e.g. private correspondence).

Marketing firms and others are increasingly using outsourced deliverability firms to better their returns on investments, or hiring full-time personnel to deal with these issues.

The publishing by ISPs of clear policies and procedures for inbound email, as well as their providing points of contact, would also serve to improve the deliverability of legitimate email.

Several of the largest receiving sites — AOL®, MSN® Hotmail and Yahoo!® — have all published policies and procedures outlining the requirements for legitimate emailers who want to be white-listed. How much this status circumvents inbound-spam filtering naturally varies between sites.

Several technical methods are currently used to fight spam. However, some of these methods may not always be able to distinguish between legitimate email and spam. For example, some spam filters block bulk mailings of legitimate emails simply because they look similar in nature to spam. Others analyze the content of email messages in order to decide whether or not to filter them, using keywords that can appear in legitimate email as well as in spam. To complicate matters further, spammers often design their emails to look like legitimate email, and also use other techniques to trick filters.

As mentioned in the "Challenge" section of this chapter, email certification is emerging as a method that could be used to help spam filters allow legitimate email through to its intended recipients. It could also allow verifiable determination between legitimate and phishing emails.

Box 4: Recommended Best Practices for Email Marketing

- Marketing email should only be sent to recipients who have provided their consent to receive such information.
- In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving all further business and/or marketing email messages from the organization.
- The internal process used to obtain consent should be clear and transparent. Organizations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.
- Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.
- Every email should provide a link to the sender's privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through "clickstream" means or other website monitoring techniques.
- Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.
- Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.
- When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.
- All email containing sexually explicit content should include the prefacing tag "SEXUALLY EXPLICIT" in the subject line.
- Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.
- Organizations may disclose the email addresses of existing customers to third-party affiliates or within a family of companies if:
  - they have consent to do so;
  - they are using the addresses for purposes consistent with their collection (i.e. marketing related to the original purchase or to provide services related to that purchase);
  - it is transparent to the recipient why they are receiving email communications; and
  - there is an easy-to-use way to opt out of receiving further email communications.

False positives are a problem, not only because they undermine the effectiveness of email as a marketing tool for businesses, but also because they cause difficulties for end-users, who are increasingly relying on the deliverability of the email they send and receive from associate sources, be they professional (e.g. business colleagues), commercial (e.g. as a result of marketing and online purchases the user has requested) or personal (e.g. private correspondence).

Marketing firms and others are increasingly using outsourced deliverability firms to better their returns on investments, or hiring full-time personnel to deal with these issues.

The publishing by ISPs of clear policies and procedures for inbound email, as well as their providing points of contact, would also serve to improve the deliverability of legitimate email.

Several of the largest receiving sites — AOL®, MSN® Hotmail and Yahoo!® — have all published policies and procedures outlining the requirements for legitimate emailers who want to be white-listed. How much this status circumvents inbound-spam filtering naturally varies between sites.

Email Certification

Several technical methods are currently used to fight spam. However, some of these methods may not always be able to distinguish between legitimate email and spam. For example, some spam filters block bulk mailings of legitimate emails simply because they look similar in nature to spam. Others analyze the content of email messages in order to decide whether or not to filter them, using keywords that can appear in legitimate email as well as in spam. To complicate matters further, spammers often design their emails to look like legitimate email, and also use other techniques to trick filters.

As mentioned in the "Challenge" section of this chapter, email certification is emerging as a method that could be used to help spam filters allow legitimate email through to its intended recipients. It could also allow verifiable determination between legitimate and phishing emails.

Working in cooperation with the ICT Standards Advisory Council of Canada, the Task Force on Spam explored the principles, business models and techniques that characterize the different certification methods currently available in the Canadian marketplace, in order to develop a reference paper that captures the results of this analysis and examines options for implementing an email certification regime in Canada.

Recommendations

Commercial emailers have the most to lose and the most to gain in the battle to stop spam. Of the various stakeholder groups involved in the fight against spam, commercial emailers also face the greatest challenges in organizing themselves to take concerted action against spammers and to play their part in implementing the toolkit approach.

A number of distinctly different kinds of organizations make up the commercial-emailers stakeholders group, including:

- companies that commission bulk commercial email in order to market their products and services;
- companies that engage in email marketing;
- companies that design and manage marketing campaigns;
- commercial-email service providers; and
- companies that supply lists of email addresses.

In some cases, the companies that provide these different kinds of products and services are vertically integrated across different segments of the commercial-email supply chain. In other cases, they are independent of each other and operate on the basis of contractual arrangements.

The majority of companies that make up the diverse population of the email stakeholder group operate according to existing laws and in conformity with generally accepted business practices. As the PIPEDA cases demonstrated, these companies are usually quick to make amends if they are found to be engaging in activities or practices that contravene these standards.

Unfortunately, each segment of the email supply chain contains spammers — companies and individuals that deliberately contravene the laws that currently prohibit sending unsolicited commercial email, or that use email as a cover for activities that are intended to deceive, cause harm to computers and network facilities, steal personal information and commit fraud.

To stop spam, it is necessary to stop spammers. If this is not done, there is a risk that Canadians will lose confidence in the Internet — not just as a vehicle for marketing and promoting products and services, but also as a method of effective communication. A general loss of confidence in email would, in turn, severely inhibit the emergence of an e-economy in Canada, and would undermine the interests of the many businesses, organizations, institutions and governments involved in the professional email supply chain.

We therefore recommend the following:

Recommendation 12:

Commercial email marketers should implement the best business practices recommended by the Task Force on Spam and should, in cooperation with the coordination body established by the Minister of Industry, monitor the effectiveness of these practices on an ongoing basis.

Recommendation 13:

Canadian industry, in coordination with international standards-development organizations, should continue to investigate various certification methodologies and their associated costs to determine which, if any, would provide the most suitable certification regime for Canada.

Recommendation 14:

To help determine the extent of the problem of non-deliverability of legitimate email in Canada, the coordination body established by the Minister of Industry should, with the help of appropriate stakeholders, formally study this issue on an ongoing basis.

5 PROMOTING PUBLIC AWARENESS

THE CHALLENGE

While there is much that lawmakers, enforcement agencies, ISPs and other network operators, and commercial emailers can do to fight spam, there is general agreement that all Internet end-users, whether they are employees, students or consumers, have an important role to play in the ongoing battle against spam.

It is also clear that, in order to help Internet users play their part, more needs to be done to inform them about what they can do to limit the amount of unwanted commercial email they receive, to protect themselves and others against viruses, to avoid falling prey to fraud and to prevent their computers from being turned into "botnets" used without the user's knowledge to send spam.

There is a considerable amount of readily available information on the steps users can take to limit the amount of spam they receive and avoid falling victim to the kinds of deceptive, fraudulent or other criminal practices associated with spam. However, public opinion surveys have demonstrated that more effort is needed to communicate this information, particularly as it pertains to emerging threats that can compromise machines, harm consumers and undermine Internet security.

Some of the simplest messages — such as "do not open unsolicited emails," "do not buy from spammers" and "do not provide personal information if you are not certain who you are dealing with" — have either not yet reached all users or not been understood. For example, the Ipsos-Reid *Ipsos Trend Report Canada* for May–June 2004 reported that more than one third of online Canadians open their spam emails, and that the main reason they give for doing so is curiosity.

A recent study by Option consommateurs also indicated that certain groups might benefit from increased education and awareness efforts tailored to their specific needs. These groups included people under 30 — who reported receiving more spam than other groups — and the elderly.

Given the low rates of positive consumer response needed to make spamming operations commercially viable, awareness of the relationship between the incidence of spam and consumer behaviour needs to be more strongly emphasized as part of the toolkit approach.

Because of their direct relationship with Internet users, ISPs and legitimate sellers of goods and services are in good positions to deliver a public education and awareness campaign in partnership with consumer groups and governments. The challenge facing the Task Force on Spam, therefore, was to facilitate the development of an appropriate social marketing and communications campaign aimed at users; and to implement it in conjunction with consumer groups, other government departments and agencies, and interested international partners.

Task Force Actions

The Task Force reviewed existing public opinion research related to consumers' views on spam, and looked at current education and awareness campaigns, both in Canada and in other countries. Many of these initiatives had enjoyed limited exposure, but in certain cases, key messages had lacked consistency. Following the review of research and initiatives, the Task Force developed a general communications strategy to identify the objectives, key audiences and necessary tools of a potential broad-based public education campaign on spam.

The "Stop Spam Here / Arrêtez le pourriel ici" Campaign

The first phase of the campaign strategy was the development of a bilingual Internet-based user-education campaign. Critical to this initiative was the development of consistent key messages and a common look, and the broad dissemination, by a wide range of partners, of three key tips to help users protect themselves and fight spam.

Working with communications and marketing experts, the Task Force on Spam developed an icon that could be hosted on partners' websites and would contain a link to user tips available at **http://stopspamhere.ca** and **http://arretezlepourrielici.ca**. Information on becoming a partner is also available at these two websites.

The Task Force enlisted both government and non-government partners to host the icon on their websites.

There has been a strong response to the "Stop Spam Here / Arrêtez le pourriel ici" campaign from organizations in the private and public sectors, as well as from the general public. Between November 25, 2004, the date the site went live, and April 2005, there were more than 500 000 unique visits to the site, and some 200 organizations joined the campaign.

Recommendations

The "Stop Spam Here / Arrêtez le pourriel ici" campaign has started a process of educating Canadian Internet users about what they can do to reduce the amount of spam they receive in their inboxes and avoid falling victim to the kinds of deceptive, malicious, fraudulent and otherwise illegal activities associated with certain kinds of spam.

However, much more needs to be done to enable Canadians to play their part in fighting spam, beginning with enhancing the "Stop Spam Here" and "Arrêtez le pourriel ici" websites, and extending the information they provide to other communications media.

General messages that apply to all consumers, of the kind in the "Three Key Tips" presented below, provide a solid foundation for raising awareness and educating the public. However, the Task Force believes that in order to make further progress it is also necessary to develop awareness and education campaigns that are targeted to the specific needs and interests of different groups in the Canadian population.

Stop Spam Here: Three Key Tips

1. Protect your computer

Spam is a growing source of computer viruses. It is critical that you protect your computer from virus-carrying messages. Install and regularly update antivirus and anti-spam software. If you don't have the extra protection of a firewall, get it.

2. Protect your email address

Reserve one email for your trusted personal and business contacts. Create a separate, expendable email address for other online uses.

3. Protect yourself

Don't try, don't buy and don't reply to spam. Just delete it. It's a great way to prevent receiving more spam in the future.

The Task Force feels that it is particularly important to engage small and medium-sized enterprises in the fight against spam, since they stand to be among the major beneficiaries of a spam-free e-commerce environment.

We therefore recommend the following:

Recommendation 15:

As part of its ongoing effort to increase user awareness and education, the federal government, in cooperation with interested stakeholders, should continue to promote the "Stop Spam Here / Arrêtez le pourriel ici" user-tips campaign by encouraging others to link to the websites, and through the use of other appropriate methods and media.

Recommendation 16:

The federal government, in cooperation with interested stakeholders, should continue to maintain and enhance the "Stop Spam Here / Arrêtez le pourriel ici" websites in order to increase their value as education tools and sources of appropriate links to other anti-spam resources, and to ensure that they remain up to date and relevant (e.g. by including information on industry best practices and future anti-spam legislation and complaints procedures).

Recommendation 17:

The federal government, in cooperation with interested stakeholders, should develop appropriate and consistent anti-spam education and awareness campaigns tailored to the needs of different target audiences.

6 ADDRESSING A GLOBAL PROBLEM

THE CHALLENGE

It has been estimated that only a small proportion of the spam received by Canadians originates in Canada. This reflects the fact that, because of the open nature of the Internet, spam can potentially be sent from anywhere, to anywhere. Stopping spam therefore requires the harmonization of anti-spam policies, and cooperation among different countries in enforcing anti-spam laws.

Canada has been active for a number of years already in international forums where Internet issues are discussed. Recently, much of this discussion has focussed on the different legislative, regulatory and enforcement actions taken by some countries to deal with spam, and the need to ensure that these approaches are compatible with the global Internet environment.

As a result of this work, progress is being made in coordinating anti-spam policies between countries, and in cooperating internationally to enforce anti-spam laws and regulations. In some cases, this has been done by piggybacking anti-spam enforcement action onto existing cooperative agreements, such as the one between Canada's Competition Bureau and the U.S. Federal Trade Commission. However, these existing arrangements have been used only to a limited extent, and new arrangements should be developed to deal specifically with anti-spam enforcement.

Much remains to be done to promote effective international coordination and collaboration in the worldwide fight against spam. While it is important to coordinate legislation, regulation and enforcement, it is now clear that a broader approach is needed at the international level. Many countries now recognize that a multistakeholder toolkit approach, of the kind Canada has consistently advocated, is proving to be the most effective approach in fighting spam and dealing with other online problems.

For this reason, the Task Force on Spam supports the development and adoption of best practices for email marketers and network management in an internationally coordinated manner. We also encourage Canadian ISPs, email marketers, business email users and Canadian consumer representatives to become active in international efforts to combat spam through initiatives such as the development of globally compatible email authentication and certification regimes.

Task Force Actions

The Task Force on Spam promoted the strong, coordinated presence by the Government of Canada and all Canadian stakeholders in developing and implementing bilateral and multilateral approaches to fighting spam. To this end, members of the Task Force were active in a number of important international forums.

Multilateral Cooperation

1) Organisation for Economic Co-operation and Development Task Force on Spam

Canada is an active participant in the Organisation for Economic Co-operation and Development Task Force on Spam, which has developed an anti-spam toolkit along lines similar to Canada's multifaceted approach.

Individual countries have volunteered to lead or participate in developing elements of the toolkit. Canada has volunteered to undertake a comparative analysis of the anti-spam legislative frameworks that are in place internationally, and has also offered contributions to a number of other items, such as public education and awareness, anti-spam technologies and industry-led measures resulting from Canada's Task Force on Spam's work, including its recommended best practices for ISPs and other network operators.

2) London Action Plan

In October 2004, representatives of the public and private sectors from 15 countries, including Canada, met in London, England, to discuss ways of improving international cooperation in enforcing anti-spam laws and regulations. Since different countries have different anti-spam legislative frameworks, the meeting brought together a broad range of enforcement agencies that may not usually work together, including agencies responsible for data- and privacy-protection, consumer protection, competition and communications regulation.

The result of this meeting was the London Action Plan on International Spam Enforcement Cooperation, which aims to develop ways and means of improving international cooperation in dealing with spam and spam-related problems.

The London Action Plan on International Spam Enforcement Cooperation does not replace international agreements that already exist between enforcement agencies. Rather, its main purpose is to enhance communication among the diverse agencies involved in the fight against spam. The Task Force indicated its support for the London Action Plan on International Spam Enforcement Cooperation, and, through Industry Canada, participated in its implementation. The Office of the Privacy Commissioner of Canada is also participating.

3) Other Multilateral Cooperation

The Task Force was involved in the anti-spam activities of the Asia–Pacific Economic Cooperation forum, the International Telecommunication Union and the World Summit on the Information Society, including in the work of the United Nations Working Group on Internet Governance.

The Task Force also supported the anti-spam activities of the United Nations Conference on Trade and Development, the Internet Engineering Task Force, and the International Consumer Protection and Enforcement Network.

The Task Force would also like to acknowledge the important work done by the private sector through bodies such as the Anti-Spam Technical Alliance, the Messaging Anti-Abuse Working Group and various industry associations.

Bilateral Initiatives

Canada is actively promoting international cooperation in the implementation of anti-spam policies and strategies through bilateral policy agreements with key partners, including Australia, the United Kingdom, the United States, Taiwan and the European Commission. Agreements have already been signed with Australia and the United Kingdom, and the Task Force anticipates that agreements will be signed later in 2005 with the United States, Taiwan and the European Commission.

Recommendations

Canada has a long history of international leadership in communications policies and strategies. In recent years, our comprehensive e-commerce policy framework, our competitive broadband marketplace, and our service-transformation and government-online initiatives have drawn international attention.

The Task Force believes Canada has an opportunity to lead in the next phase of the global fight against spam. Although a number of other countries have already enacted anti-spam legislation, and were the first to promote cooperative enforcement mechanisms, Canada has seen demonstrated results in industry best practices and its public awareness campaign, which are solid first steps demonstrating the value of adopting a multifaceted, multistakeholder approach that complements strong laws and vigorous enforcement with other tools.

As well as an opportunity, the Task Force believes Canada has an obligation to exercise international leadership in combatting spam. One major contribution the country can make is to reduce the amount of spamming in Canada.

In analyzing the experiences of other countries and the efforts currently under way to construct cooperative enforcement mechanisms, the Task Force has come to the following conclusions.

- There is much to be learned from the experience of other countries about what works — and what does not work — in the fight against spam and related threats to the Internet. As well as reinforcing the importance of adopting a multistakeholder toolkit approach, these experiences demonstrate the importance of founding the fight against spam on laws that prohibit sending commercial email without the prior consent of the intended recipients, and that provide significant penalties for engaging in spamming activities.

- The actions that we take within Canada to reduce the amount of spam will only have a limited effect on the amount of spam arriving in Canadians' email inboxes, unless these actions are complemented and reinforced by strong, effective international cooperative actions against spammers.

- Canada has an opportunity to lead in the growing international fight against spam, particularly by helping developing countries adopt a multistakeholder toolkit approach to fighting spam and adapt it to their own needs and capabilities.

We therefore recommend the following:

Recommendation 18:

The federal government should continue to pursue bilateral agreements on anti-spam policies and strategies with foreign governments.

Recommendation 19:

The federal government, in consultation, collaboration and partnership with other stakeholders as appropriate, should actively promote and assist the coordinated international implementation of anti-spam policies, laws, regulations and enforcement measures; industry standards and practices; and public education and awareness activities.

Recommendation 20:

Canada should make its expertise in developing multistakeholder toolkit approaches to combatting spam available to help developing countries.

7 COORDINATING FUTURE ACTION

THE CHALLENGE

Success in implementing Canada's multistakeholder, multifaceted strategy for combatting spam and related threats to Internet security requires a highly synchronized, coordinated approach to spam prevention and enforcement. In enforcement, in particular, the work of the Task Force on Spam has revealed the need for more effective communications, cooperation and collaboration, as there are many law enforcement and regulatory bodies, each with partial responsibility for fighting spam.

The toolkit approach was adopted because of the complex nature of the spam problem. This complexity will not change after the Task Force completes its mandate. Going forward, the government and other stakeholders will face the same set of challenges that led to the establishment of the Task Force. Examples of these challenges include the following:

- There will be continuing issues surrounding the enforcement of anti-spam laws, including coordination between different agencies and different jurisdictions, the need for adequate technical expertise to conduct investigations and the availability of dedicated resources to successfully prosecute perpetrators.
- ISPs and other network operators will have a continued need to share information on best practices and effective strategies to counter emerging threats, as well as to develop sound metrics to measure the scope of the spam problem in Canada and the effectiveness of anti-spam measures.
- Canada's Internet users will have an ongoing need for reliable, accurate information on how to protect themselves from spam and the deceptive, malicious and fraudulent practices associated with spam. They will also continue to need a focal point where complaints can be made through a simple process.
- There will be a continuing and increasing need to coordinate participation by Canadian stakeholders in the international fight against spam.

Task Force Actions

Taking into account its own experience and the experiences of other countries, the Task Force on Spam came to the conclusion that, in order to respond successfully to spam-related challenges, the Government of Canada must establish or designate a focal point or centre to lead the fight against spam and related threats. This centre should be responsible for two main functions: policy oversight and coordination, and support to enforcement agencies.

To be an effective focal point for ongoing policy development and coordination, the Task Force believes the centre should have the mandate and resources to:

- develop policy approaches to deal with the issue of spam and related threats — including through monitoring and analyzing issues, and maintaining ongoing consultations with key stakeholders;

- collect and compile information and statistical data for measuring and benchmarking the scope of the spam problem in Canada and the effectiveness of anti-spam measures, including the two sets of best practices developed by the Task Force and the "Stop Spam Here / Arrêtez le pourriel ici" campaign;
- provide the public with information and other resources, as well as support and referral services, to help Canadians keep themselves safe from spam; and
- encourage international and domestic public and private sector and academic collaboration in the fight against spam.

In order to effectively support a nationally and internationally coordinated approach to anti-spam law enforcement, the Task Force believes the centre should have the mandate and resources to:

- receive, analyze and refer complaints from the public about spam and related activities;
- refer cases and supporting evidence to the appropriate law enforcement or regulatory agencies; and
- provide technical expertise in support of prospective and ongoing investigations.

The Task Force examined a number of possible organizational models, including Canadian models, such as PhoneBusters and the National Child Exploitation Coordination Centre, and U.S. models, such as Operation Slam Spam and the AntiPhishing Working Group. However, it was clear from our examination that none of these models would meet all of the requirements associated with the centre's dual mandate as we envision it.

Essentially, three different options exist for establishing such a centre:

1) creating a new public–private partnership outside of government;

2) locating the centre in a federal government department; or

3) assigning the responsibilities to an existing regulatory agency.

Since the Minister of Industry would be responsible for anti-spam legislation, the Task Force has come to the conclusion that establishing the centre under Industry Canada would be the preferred approach. In our view, a body attached to a federal department would be best positioned to perform the necessary policy oversight, coordination and advisory functions most effectively.

Moreover, the need for active ongoing collaboration with the private sector to operate the "Spam Freezer" and exchange spam information in real time might be more easily met by a departmental body rather than by an agency with a regulatory or semijudicial role. In that context, the Task Force underlines the importance of involving the private sector in the operation of the centre, and including industry and consumer voices in its governance.

Recommendations

It is clear that a multistakeholder toolkit approach to fighting spam will not work over the longer term unless there is a body of some kind that has the responsibility, the authority and the technical resources required to coordinate this fight.

It is also clear that it will be necessary for the Government of Canada to periodically review the extent to which stakeholders have implemented the Task Force's recommendations, measure the success of the multistakeholder approach in reducing spam and assess the effectiveness of Canada's anti-spam strategy in light of emerging threats.

We therefore recommend the following:

Recommendation 21:

In order to carry forward the multi-faceted, multistakeholder approach that has been developed by the Task Force on Spam, and to provide a focal point for facilitating the implementation of its recommendations, the federal government should establish a centre, reporting to the Minister of Industry, responsible for policy oversight and coordination, public education and awareness, and providing support to enforcement agencies.

Recommendation 22:

The federal government, through this coordinating body, should monitor the impact of the implementation of the Task Force's recommendations; evaluate the results; provide regular public reports; and, in consultation with stakeholders, take whatever additional measures are necessary to combat spam.

APPENDICES

APPENDIX A

MEMBERS OF THE TASK FORCE WORKING GROUPS AND SECRETARIAT

Legislation and Enforcement

Co-chairs

Michael Geist, Canadian Research Chair in Internet and E-Commerce Law, University of Ottawa
Roger Tassé, Partner, Gowling Lafleur Henderson LLP

Member Organizations

Amazon.com
Bell Canada
Canadian Cable Telecommunications Association
Canadian Coalition Against Unsolicited Commercial Email
Canadian Internet Policy and Public Interest Clinic
Canadian Radio-television and Telecommunications Commission
Canadian Wireless Telecommunications Association
Cogeco Cable Inc.
Competition Bureau
First Data Corporation
Information Technology Association of Canada
Justice Canada
LinuxMagic
Microsoft Canada
Nortel Networks
Office of Consumer Affairs, Industry Canada
Office of the Privacy Commissioner of Canada
PayPal Inc.
Rogers Communications Inc.
Royal Canadian Mounted Police
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
TELUS Communications Inc.

Network and Technology Management

Co-chairs

Tom Copeland, President, Canadian Association of Internet Providers
Lori Assheton-Smith, Senior Vice-President and General Counsel, Canadian Cable Telecommunications Association

Member Organizations

Allstream
AOL Canada
Bell Canada
BorderWare Technologies Inc.
Canadian Coalition Against Unsolicited Commercial Email
Canadian Internet Registration Authority
Canadian Wireless Telecommunications Association
CANARIE Inc.
Chief Information Office, Industry Canada
CipherTrust
Cogeco Cable Inc.
Delta Cable Communications
E-Gate Communications Inc.
easyDNS Technologies Inc.
Group Telecom
Interlink Connectivity
Internet Light and Power
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
LinuxMagic
MessageLabs Americas
Microsoft Canada
Nortel Networks
PhoneBusters
Rogers Communications Inc.
SecuritySage Inc.
Shaw Communications Inc.
Spamhaus
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
TELUS Communications Inc.
University of British Columbia
University of Manitoba
Videotron Telecom Ltd.
Vircom Inc.

Validating Commercial Email

Co-chairs

Neil Schwartzman, Chair, Canadian Coalition Against Unsolicited Commercial Email
Amanda Maltby, Senior Vice President, Ipsos-Reid Public Affairs, Representing the Canadian Marketing Association

Member Organizations

24/7 Canada Inc.
AOL Canada
Bell Canada
Canadian Cable Telecommunications Association
Canadian Marketing Association
Cornerstone Group of Companies
Daemon Defense Systems
Digital Cement
Doubleclick
eBay Inc.
ICT Standards Advisory Council of Canada (ISACC)
Information Technology Association of Canada
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
MS Planners
Office of Consumer Affairs, Industry Canada
Partners Inc.
Rogers Communications Inc.
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
Technology Surveys International

Public Education and Awareness

Co-chairs

Suzanne Morin, Assistant General Counsel, Regulatory Law and Policy, Bell Canada
Geneviève Reed, Head of Research and Representation, Option consommateurs

Member Organizations

Bell Canada
Canadian Association of Internet Providers
Canadian Coalition Against Unsolicited Commercial Email
Canadian Internet Policy and Public Interest Clinic
Chief Information Office, Industry Canada
Competition Bureau
Consumers Council of Canada
Information Technology Association of Canada
Media Awareness Network
Office of Consumer Affairs, Industry Canada
Office of the Privacy Commissioner of Canada
Openface Internet Inc.
Public Interest Advocacy Centre
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
The Canadian Chamber of Commerce
Union des consommateurs

International Collaboration

Co-chairs

Bernard Courtois, President, Information Technology Association of Canada
Michael Geist, Canadian Research Chair in Internet and E-Commerce Law, University of Ottawa

Member Organizations

Bell Canada
Competition Bureau
Department of Communications, Information Technology and the Arts, Australia
Department of Trade and Industry, United Kingdom
European Commission
LinuxMagic
Microsoft Canada
Organisation for Economic Co-operation and Development
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
The Canadian Chamber of Commerce

Task Force Secretariat

Spectrum, Information Technologies and Telecommunications Sector, Industry Canada

Richard Simpson, Director General, Electronic Commerce Branch
Shari Scott, Director, Electronic Commerce Branch
David Charter, Electronic Commerce Branch
Gérard Desroches, Electronic Commerce Branch
Peter Ferguson, Electronic Commerce Branch
Lisa Foley, Electronic Commerce Branch
Angie Forte, Electronic Commerce Branch
Jennifer Kealey, Electronic Commerce Branch
Serge Presseau, Electronic Commerce Branch
Howard Chatterton, Spectrum Engineering Branch
David Gibson, Spectrum Engineering Branch

Don MacLean, MacLean Consulting, Report Author
John Levine, Glossary Author and Technical Editor

APPENDIX B

RECOMMENDED BEST PRACTICES FOR INTERNET SERVICE PROVIDERS AND OTHER NETWORK OPERATORS

Background

In August 2004, the Working Group on Technology and Network Management started developing a number of technical best practices that would contribute to the reduction of email spam. The Working Group's mandate represents a continuation of the efforts and progress that have been under way for some time, in Canada and internationally, including the work of the Anti-Spam Technical Alliance (ASTA) and the Messaging Anti-Abuse Working Group (MAAWG), and the efforts of various industry associations. A number of different ISPs, other network operators, technical groups and forums have been working collaboratively for many months to share best practices for reducing spam.

The Working Group on Technology and Network Management did not try to redo work that had already been done. Rather, it sought to bring the various industry groups together to share the results of work already under way, and to encourage the broad adoption of best practices among ISPs, other network operators and large enterprise users.

The Working Group emphasizes that the widespread adoption of these best practices will not, in and of themselves, constitute a comprehensive solution to spam. They are, however, part of a broader, multi-prong strategy for addressing the problem of spam.

Intent

The Working Group's recommendations for best industry practices to combat spam are voluntary. The actual time frames for their implementation may vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. In some cases, alternative solutions may achieve the same objectives outlined in the recommendations. The selection of solutions is at the discretion of the provider/operator.

The Working Group supports all efforts to combat spam. Flexibility in the implementation of the recommended best practices is the key to achieving their broad and meaningful adoption by service providers of all sizes. Because of the technical nature of these recommendations, and the rapid pace of technological change, the Working Group is strongly of the view that these recommended best practices should not be codified as mandatory requirements.

Recommended Best Practices and Rationales

Following are the recommended anti-spam best practices for Canadian Internet service providers and other network operators, as well as a rationale for each recommendation.

1. **All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.**

The purpose of email-sender authentication is to reduce domain-name spoofing in email, thereby reducing the incidence of spamming and phishing attempts.

Methods of sender authentication are continuing to be evaluated by the Internet Engineering Task Force (IETF). At this point in time, the SPF classic (SPFv1) proposal is the most technically mature and widely deployed sender-authentication scheme.

This recommendation does not preclude the use of other methods to authenticate email messages (e.g. sender ID, domain keys, SPF, identified Internet mail, etc.). Standards will continue to develop within the industry.

2. **ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive mail over port 25 should be restricted to hosts on the provider's network. Use of port 25 by end-users should be permitted on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.**

Most ISPs and other network operators agree that there is no practical reason for dial-up / dynamic IP-address ranges to have email servers at the customer end.

There are a variety of ways to avoid this. Through their own network management, ISPs and other network operators can block the use of port 25 on an egress basis.

It has been the experience of members of the Working Group that blocking port 25 affects very few users, and that these users can usually be accommodated in other ways.

The benefits of blocking port 25 are frequently dramatic — some ISPs have seen a 95-percent drop in virus emissions, a 98-percent drop in abuse reports, a reduction in internal viruses / compromised machines used to send spam and attendant cost savings in abuse-related network management.

3. **ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.**

Many viruses and worms are carried by file attachments. Blocking email containing problematic attachments would have little impact on users. The most common file extensions carrying a payload are: .pif, .scr, .exe and .vbs.

Many ISPs and other network operators should filter attachments based on their properties (i.e. infections) versus extension names. This is a matter of resource availability. Since some business or technical users may have legitimate reasons for sending .exe or .vbs files, filtering for content may be more efficient than filtering for extension names.

4. ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.

Monitoring and possibly rate-limiting the amount of email that can be sent from a particular user would be useful in discouraging spammers from using provider networks as their launching points. It would also provide an early indication of the possible infection of user machines.

Some providers currently do a limited amount of rate-limiting. Techniques will vary depending on the email server in use.

5. ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.

Using viruses, worms and malicious software, hackers and spammers have intentionally deposited millions of "back-door" open relays and proxies on the personal computers of unsuspecting users. The spammer community uses this network of compromised devices to generate billions of unsolicited email messages. In addition, hackers have used this network of devices to mount distributed denial of service (DDoS) attacks on websites, register fraudulent accounts and lay the groundwork for future anonymous hacking activities.

There are a number of methods that can be used to address compromised devices, from suspending client accounts to isolation or quarantine from the network.

6. ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.

The Working Group on Technology and Network Management is developing a list of ISPs and other operator contacts. It would be beneficial for operators to have common response expectations when reporting incidents of significant network abuse to other network operators. Escalation processes within companies would remain a proprietary process, but initial intercompany communications need a common "estimated time to recovery."

7. ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.

This is to ensure that subscribers are well aware of their ISPs', other network operators', and/or enterprise email providers' security policies and procedures. It will be particularly important to relay information related to recommendations #2, #3 and #5.

Another Task Force working group, the Working Group on Public Education and Awareness, has developed a multistakeholder public information and awareness campaign to educate, most specifically, Canadian end-users about what they can do to limit the amount of unwanted commercial email they receive.

8. **ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).**

Email validation would ensure that only authenticated clients are allowed to send email via the server. For example, SMTP authentication is an enhancement to SMTP servers to enable them to verify the identity of email clients. The protocol works by requesting the user name and password of the email sender and validating this against preregistered clients. This procedure can be used to reduce spam messages, since these messages are unlikely to be from registered users in the SMTP authorization list.

9. **Non-delivery notices (NDNs) should only be sent for legitimate emails.**

Message transfer agent (MTA) administrators and spam-filter manufacturers have now generally accepted this practice. When a message is sent to a nonexistent user account, the MTA responds stating that the user does not exist. This can cause problems when a spammer spoofs a large number of addresses from a domain. Each nonexistent address generates a non-delivery response from the mail server. The MTA software should be configured not to send non-delivery messages for spoofed addresses.

Blanket cessation of NDNs may, however, create some problems for users who, for example, have mistyped an email address and are assuming that the message reached its destination.

10. **ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.**

Identifying the points of contact for ISPs and network operators is crucial for managing the abuse of email communication systems. All email messages include information such as DNS host names, IP addresses and other records relating to the source, transmission and destination of the message. The ISPs or other network operators responsible for sources of the email messages should be easily and accurately identifiable. All fully qualified domain names(e.g. hostname.domainname.ca), domain names and IP addresses should be registered and maintained with information allowing such identification.

Network operators should also ensure that domain name records; forward and reverse DNS records; and WHOIS, shared WHOIS Project (i.e. SWIP) or referral WHOIS (i.e. RWHOIS) records are responsibly maintained with correct, complete and current information. For example, American Registry for Internet Numbers WHOIS records should include an OrgAbuseHandle including contact information for those responsible for managing abuse originating in that network. ISPs and network operators are responsible for maintaining registration information, DNS records and other identifying information in accordance with the relevant Request for Comments (RFCs) such as RFC 2142 — Mailbox Names for Common Services, Roles and Functions.

11. **ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.**

Forged email-header information is common in spam and email malware. Ensuring that all publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS, WHOIS and SWIP registration records is very important for being able to identify the sources of email and other online communication methods. Identification of the source provides the information required to contact the responsible ISPs or other network operators, so that they can take appropriate actions to address spam or other concerns involving protocol. IP addresses registered to another organization should not be used within private networks, as their use can significantly complicate efforts to identify the ISPs and network operators responsible for an email message. DNS host names may also be used by recipients to determine access policy, but should be chosen carefully in order to avoid recipients choosing overly broad filtering policies that have the potential to block valid email. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

To assist with identification of email sources, it is also suggested that email servers should have DNS host names that clearly differentiate these servers from consumer or business desktop addresses. Host names should exist and match in both forward (resolution of host name to IP address) and reverse (resolution of IP address to host name) DNS entries. ISP customers who are permitted by policy to operate email or other servers will benefit from this by having the ability to operate customized forward and reverse DNS within their domains, thus distinguishing hosts from residential or policy-prohibited hosts. This lets email recipients establish systems that differentiate between legitimate email servers and hosts that may be sources of spam.

Residential, dynamic or policy-restricted IP addresses should also have a clear and consistent forward and reverse DNS naming convention. For example, access-control policies enacted by email recipients which differentiate between trusted and untrusted email sources are easier to establish for naming conventions that include the domain owner; service class; static or dynamic assignment; and other identifiers, such as an IP-pool identification. This can prevent ISP customers who are permitted to run email servers from being blocked due to their being indistinguishable from illegitimate email sources. Naming conventions with a "most-significant-to-the-right" scheme simplify filters and reduce the likelihood of access-control policies affecting legitimate email sources. For example, such a naming convention for the residential, dynamic IP address "1.2.3.4" at ISP Example.ca would be "4-3-2-1.dyn.res.example.ca." A sample naming convention for the small business, static IP address "1.2.3.4" at ISP Example.ca would be "4-3-2-1.static.bus.example.ca." A sample naming convention for an email server used by Smallbizcustomer.ca would be "mail.smallbizcustomer.ca."

12. **ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822, and reference domains and IP addresses should have up-to-date, accurate registration information.**

Accurate email-header information is important for ISPs and other network operators to be able to identify sources of spam and email malware within an ISP's network. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

While internal networks will often use private IP addresses (as per RFC 1918 — Address Allocation for Private Internets) that are not externally routable or identifiable, email providers should ensure that the sources of email messages are accurately identifiable for policy- and law-enforcement purposes.

Conclusion

Spam is a multifaceted, global problem that requires coordinated action on several fronts in order to achieve real and measurable progress. Implementing these recommendations can help reduce many of the worst types of spam, forgery and spoofing that occur in email. These measures will not stop spam entirely, but will significantly enhance the Internet community's ability to trace the sources of spam and hold senders accountable for their actions. The recommendations are also expected to provide the foundation on which future solutions can be built.

APPENDIX C

RECOMMENDED BEST PRACTICES FOR EMAIL MARKETING

Background

As part of the federal government's Task Force on Spam, the Working Group on Validating Commerical Email has developed a set of best practices for email marketing. These best practices will help Canadian organizations adopt spam-free marketing techniques and will make it clear that spam plays no legitimate role in Canadian marketing.

Most responsible organizations already follow industry codes or have adopted best practices. In Canada, organizations are guided by the Canadian Marketing Association's *Code of Ethics and Standards of Practice*, which includes guidelines for email marketing and the online collection of data for marketing purposes. Members of Canadian Survey Research Council organizations that conduct online surveys are also developing a uniform code of practice.

This document brings together a set of best practices drawing upon existing codes in order to provide all with a basis to using email for commercial or marketing purposes.

Increasingly, Internet service providers (ISPs) and email service providers (ESPs) are looking for ways to stop spam by using filtering, black and white lists. As a result, they are inadvertently blocking legitimate email messages before they reach their intended recipients. Organizations are encouraged to adopt the best practices cited here as a way to ensure that their own legitimate email messages reach their intended recipients.

These best practices are not legally binding, but are intended to complement existing Canadian laws that govern spam, privacy, email marketing and marketing to children. For example, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into full force throughout Canada in January 2004, establishes the obligations of those who collect, use and disclose personal electronic-mail addresses. Other relevant federal acts include the *Competition Act*, the *Telecommunications Act* and the *Criminal Code* of Canada. Organizations should make themselves aware of these laws and govern their activities accordingly.

The best practices, along with explanatory notes and illustrative examples, are outlined in the following sections.

Recommended Best Practices

1. Marketing email should only be sent to recipients who have provided their consent to receive such information.

This best practice directly relates to the sending of unsolicited commercial email for the purposes of soliciting goods and/or services. If organizations have not obtained the express consent of recipients prior to sending these types of email messages, then they are sending spam.

If the organization has an existing business relationship (see glossary) with the intended recipient, it is sufficient to rely on implied consent. Under existing Canadian law, where an individual has entered a contest, made a donation, or registered online for a product, newsletter, etc.; has provided their email address as part of the transaction; and has been provided with the opportunity to opt out of receiving further marketing email messages, and has not done so, the organization has the implied consent to

email the individual. When using this form of consent, the marketer should explain to the intended recipient why they are receiving the email. In the follow-up communications, the organization must provide the individual with an opportunity to opt out of receiving further marketing emails (see Best Practice #2).

Organizations should not send email marketing messages to recipients who have indicated they do not wish to receive email messages from the organization. While an organization may send email messages during an existing business relationship, they must honour an individual's request to be removed from email marketing lists at any time. This can be accomplished by providing an opt-out opportunity in every message sent (see Best Practice #2).

There is an exception for sending email messages outside of an existing business relationship, or to a customer whose file has become inactive. If the organization has service, warranty or product-upgrade information, or if there are health and safety issues related to a product purchase, the organization may send email messages to its customers. Organizations should use discretion in doing so, however, as customers may view this email as spam if the organization uses it as an opportunity to up-sell or cross-sell products.

2. **In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving any further business and/or marketing email messages from the organization.**

In all email messages to current customers, organizations must include an opportunity for the recipient to opt out. This opportunity should not be buried in the email message and must, at minimum, be website- and/or email-enabled. The language used should be as simple as: "If you no longer wish to receive marketing offers from this organization, please **click here** or email **info@ABCcompany.com**."

The process for opting out should be simple and straightforward, and organizations should confirm by email that the opt-out request has been or will be followed through without requiring further action by the consumer.

In Canada, the industry best practice for telephone or mail do-not-contact files is to honour opt-out requests for a three-year period. After that time, organizations may re-contact individuals with marketing offers. However, because of the sensitivities associated with email communications, and the problems caused by spam, organizations should honour an email opt-out request as final and remove that individual from their marketing lists until such time as the individual opts to receive email messages again.

3. **The internal process used to obtain consent should be clear and transparent. Organizations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.**

Organizations should ensure that they have the means to honour opt-out requests on a timely basis and to scrub their lists accordingly.

In addition, an internal process should be in place that records proof of consent, including the date, time, originating Internet protocol (IP) address and location (including URL), where the address collection occurred and whether consent was obtained via another medium (e.g. business card, contest form, telephone, verbal communication or credit card [e.g. through a paying subscription to a list]). Organizations should be able to provide this information to a recipient upon request.

4. Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.

The identification of the sender and source of the email should be clearly and obviously specified and, whenever possible, placed above the fold (that part of the email that is visible without scrolling).

Example #1: Direct from organization to subscriber

Date: Tue, 5 Oct 2004 07:32:02 -0400
From: Bell Canada - Electronic bill <bill.presentment@bell.ca>
To: JOE CONSUMER"<joe@consumer.ca>
Subject: Your Bell e-bill is ready / Votre facture électronique est prête

Example #2: Third-party email service provider to subscriber on behalf of an organization

From: "peteMOSS PUBLICATIONS <bounces@peteMOSS.com>"
<v2user-13990-IXoyuP..CahrNet_0bkttg@mailer.whitehat.com>
Subject: spamNEWS 07/21/04
To: <joe@consumer.ca>
Date: Sat, 24 Jul 2004 18:50:17 -0700

Even in cases where the content is accurately related to the subject line, organizations are cautioned against using subject lines that refer to "free offers" or "winning prizes." This is, in part, due to the fact that some spam filters use keywords such as these to signal that the message is spam.

Email messages should include the sender's main postal address. Canadian organizations are strongly encouraged to become familiar with the provisions in Canadian laws that address this issue, and with the related laws of other jurisdictions, such as Australia, the United States and the European Union.

5. Every email should provide a link to the sender's privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through "clickstream" means or other website monitoring techniques.

Organizations are obliged under PIPEDA to adopt a significant degree of transparency in disclosing their personal-information gathering and handling practices. A privacy policy might include the type of information collected and/or used; whether information is disclosed to third parties; the use of "cookies" or other passive means of data collection; and security, accountability and enforcement procedures.

Organizations must make the information on their online information-gathering processes readily available in one comprehensive privacy policy on their websites. The privacy policy should also include an active link to an opt-out mechanism.

6. Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.

Organizations, list brokers and list owners should share responsibility for sending email to recipients who have not given appropriate consent to receive these messages. Where an organization, list broker or list owner knew or should have known that the proper consent was not obtained, they could be accountable. Some examples of reasonable steps that an organization can take to ensure clean lists include:

- reviewing the privacy policy of the broker/owner of the list;
- reviewing the opt-in procedures used to obtain the email addresses;
- having the broker or owner sign a contract warranting that they have complied with the requirements of PIPEDA (see the sample at the end of this appendix).

7. Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.

Organizations should refer to both the Canadian Marketing Association's Special Considerations in Marketing to Children and Teenagers, from its *Code of Ethics and Standards of Practice* (**www.the-cma.org/consumer/ethics.cfm**), and existing Canadian laws (see **www.justice.gc.ca**) for guidance on this issue.

The ways in which those under the age of majority perceive and react to email marketing communications are influenced by their age and experience, and the context in which the message is framed. For example, email marketing communications that are acceptable for teenagers will not necessarily be acceptable for younger children. There is no way to guarantee the age of any person who signs up to an email subscriber list. Organizations should, therefore, use discretion and sensitivity when marketing to those under the age of majority, and should seek to engage parental permission in such communications.

8. (a) When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.

Adult content includes material of a sexually explicit nature and material related to gaming and gambling, tobacco, alcohol, firearms and other weapons.

(b) All email containing sexually explicit content should include the prefacing tag "SEXUALLY EXPLICIT" in the subject line.

For example, the subscriber may be required to provide a telephone number so the organization can verify that the recipient is of the age of majority. It is important to note that contracts with minors are not enforceable.

9. Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.

Any complaints from individuals regarding the use of their email address should be dealt with courteously and within a reasonable time frame.

10. Organizations may disclose the email addresses of existing customers to third-party affiliates or within a family of companies if:

(i) they have consent to do so;

(ii) they are using the addresses for purposes consistent with their collection (i.e. for marketing related to the original purchase or to provide services related to that purchase);

(iii) it is transparent to the recipient why they are receiving email communications; and

(iv) there is an easy-to-use way to opt out of receiving further email communications.

Organizations may only disclose customers' email addresses to an affiliated third party or within a family of companies for cross-marketing purposes if they offer these customers an easy-to-use opt-out opportunity before disclosing the email address.

It must be transparent to customers why they are receiving additional, related marketing offers (e.g. under a company brand). The organization should not assume that customers understand a corporate relationship or structure.

For further guidance, organizations are advised to follow the best practices established by the Canadian Marketing Association in its *Code of Ethics and Standards of Practice* under Section E4.1.3 of the *E-mail Marketing Communications* compliance guide. The section states that "an individual's email address may not be disclosed to any third party (e.g. list rental company) without the express consent (more commonly known as opt-in or positive consent) of the individual. If you want to disclose email addresses to marketing partners or list brokers, you must obtain positive consent. Similarly, you need to ensure appropriate permission for the use of any email addresses your company may have acquired from others."

The CMA defines a "third party" as follows:

> "Third party" refers to an organization corporately distinct from that with which the customer originally did business (list rental company), including an organization corporately related to the original organizations (or charity) or part of the same group, where the relationship would not be apparent to the customer. Third parties do not include data processors operating on behalf of the organization with whom the individual has established a business relationship.

Technical Tips for Electronic Marketers

1. Sending parties should implement the following standard technical specifications:

- All servers (e.g. inbound, outbound, websites) must have reverse Domain Name System pointer (rDNS PTR) entries in DNS records, the forward and reverse DNS lookups for the host must match, and the sending machines should HELO/EHLO with this name.
- Sender Policy Framework (SPF) (e.g. **http://spf.pobox.com**) and domain-key (e.g. **http://antispam.yahoo.com/domainkeys**) records should be published by the senders and third-party sites associated with a mailing (e.g. websites, ESPs, etc.) and kept current at all times. Adoption of technologies that are similar in nature should be considered as they develop and become standardized.
- IP addresses that are distinct from other site servers should be assigned to outbound mail servers.
- WHOIS database records for all sender domains must be kept accurate and complete.
- Role accounts (e.g. postmaster@ and abuse@) must be functional and actively monitored for all sender domains, including websites, referenced in email content.

2. Senders must attend to bounce messages as follows:

- They must promptly remove "hard" (5xx — No such user / Mailbox unavailable, etc.) bounced addresses from all lists under their control when the total number of refusals surpasses three or more in fourteen days. If a 5xx bounce indicates spam blocking, the address may be reactivated if the spam block is removed.
- They must remove "soft" (4xx — Transient failures) bounced addresses when the total number of refusals surpasses five in consecutive campaigns from a single list, or five in aggregate from several lists within ten days.

Bounce-handling policies are explained in depth at the following sites:

- **http://help.yahoo.com/help/us/mail/defer**
- **www.isipp.com/standards.php**
- **http://postmaster.info.aol.com/guidelines/bestprac.html**

3. Web bugs (hidden HTML elements) and return receipts are inaccurate ways to determine open rate statistics for campaigns. Senders are strongly encouraged to cease using them and adopt alternative performance metrics.

Web bugs or web beacons have become extremely inaccurate as measurements for the effectiveness of email campaigns, and their use is discouraged.

Web beacons are no longer reliably accurate for several reasons, which mainly involve technical changes in popular client email software (e.g. as part of its antivirus security measures, Outlook will no longer download such items by default or show them in the preview pane). There is also increased use of client-side antivirus software, which, by default, disallows web-beacon downloading.

Relying on 1x1 pixel, white-on-white graphic elements as a way to measure open rates is also discouraged. The use of user click-throughs of encoded, embedded URLs and other forms of measuring subscriber actions (e.g. returns on investments, purchase actions) is advised.

If senders are going to use web beacons, the privacy implications raised in studies such as the one published by the Network Advertising Initiative (**www.networkadvertising.org/Web_Beacons_11-1-04.pdf**) should be seriously considered, and the conditions set out therein should be implemented.

Currently, one of the best measurements to look at when assessing the success of an email program is subscriber retention — that is, how many people continue to subscribe after each email. Clearly, the goal is to have no unsubscribers, which would indicate that the organization is providing content that is timely, relevant and valued. In turn, these benefits build loyalty and trust among customers — a good thing for any organization.

Sample Letter of Compliance with the *Personal Information Protection and Electronic Documents Act*

List Name: _____

As a leader in list brokerage services, **ABCcompany** takes pride in its commitment to protecting consumer privacy and ensuring compliance with applicable legislation, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA). We are, therefore, taking this opportunity to update the information we have about the list referenced above.

A Review of PIPEDA and Consumer Privacy
PIPEDA addresses consumer records only (those going to a home address). Among other things, the legislation states that consumers on a list must have provided their consent (opt-in) for the collection of their personal information and its disclosure to outside parties for marketing and/or communications purposes. Additionally, it mandates that name-removal options (opt-out) available to consumers be put into effect prior to consumers' names being released for marketing purposes.

What We Need
Increasingly, mailers are asking for specific information about the privacy messaging being used by list owners. Accordingly, we need to have the following information on record to ensure that orders are processed expediently.

Please provide a sample copy of the consent form or name-removal option currently in use. We will keep a copy on file for future reference for potential and repeat uses of this list.

Please check one of the boxes below, then sign, date and return this document to the attention of **ABCcompany** at fax number (XXX) XXX-XXXX. Please contact our XXXXXXXXX department at (XXX) XXX-XXXX or **info@ABCcompany.com** with any questions.

[ ] I warrant and represent that this list IS COMPLIANT with PIPEDA. My organization has obtained consent from all consumers on this list to collect their personal information and disclose it to outside parties for marketing and/or communication purposes, and has ensured that name-removal options are available to consumers prior to these consumers' names being released for marketing purposes. My organization shall comply with all legislation, provincial and federal, pertaining to the protection of personal information that may come into force from this date forward, as it applies to personal information collected, used or disclosed by my organization.

[ ] I warrant and represent that this list IS NOT COMPLIANT with PIPEDA. My organization has not obtained consent from all consumers on this list to collect their personal information and disclose it to outside parties for marketing and/or communication purposes, and/or has not ensured that name-removal options are available to consumers prior to these consumers' names being released for marketing purposes.

APPENDIX D

THREE KEY TIPS FOR COMBATTING SPAM

Spam refers to unsolicited email, mostly commercial, advertising a product or service that is mass mailed to thousands of email addresses at a time, filling people's inboxes. Spam does not refer to legitimate commercial email for which consumers have given their consent. Spam is often a source of scams, viruses and offensive content.

Spam is a major problem that takes up valuable time and increases costs for consumers, business and governments. Each of us must do our part to protect ourselves and others from spam. **Canada's Task Force on Spam** has developed these three tips to help you protect yourself and fight spam.

Stop Spam Here: Three Key Tips

1. Protect your computer

Spam is a growing source of computer viruses. It is critical that you protect your computer from virus-carrying messages. Install and regularly update antivirus and anti-spam software. If you don't have the extra protection of a firewall, get it.

2. Protect your email address

Reserve one email for your trusted personal and business contacts. Create a separate, expendable email address for other online uses.

3. Protect yourself

Don't try, don't buy and don't reply to spam. Just delete it. It's a great way to prevent receiving more spam in the future.

1. Protect your computer

Shield your computer with anti-spam and antivirus programs, and other security software.

Anti-spam software can automatically scan your email for spam before it gets to your inbox, sending it to a junk email box instead. This prevents you or a family member from inadvertently opening spam messages, and helps you manage your email more effectively.

To protect against virus-laden spam emails and attachments, install security patches and antivirus programs on your operating system and update them regularly.

A firewall provides added protection from hackers by protecting your privacy and personal information.

Never go online with any computer before it has had anti-spam, antivirus and firewall protection installed.

Always question the source.

Never open attachments unless you are expecting them from someone you trust. Spammers can hijack the personal and corporate email accounts of others — a process known as "spoofing" — to send viruses that can corrupt your computer. If you are in doubt about an attachment, verify with the sender before opening it.

Don't let your computer become a spam zombie.

Without the system protection listed here, your computer could be infected with viruses that are programmed to create gateways (known technically as *proxies*) that relay spam to other email recipients. In severe cases, your Internet service provider (ISP) may have to shut down your account. An infected computer can cost hundreds — or even thousands — of dollars to repair.

When completing a session on the Internet, it is a good idea to disconnect from the Internet and shut down your system. Spammers are increasingly seeking out and exploiting unprotected home computers with high-speed Internet connections to use as "spam zombies."

2. Protect your email address

Manage your online risks.

Use separate email addresses for different online activities: create one email address and share it *only* with trusted personal and business contacts. Create expendable email addresses for other online activities. If these email addresses become clogged with spam, discard them.

Select an email address consisting of a combination of letters and numbers. By choosing a more complex email address, you are making it more difficult for spammers to randomly discover and fill your email account using software that randomly combines people's first and last names.

Stay under cover.

Posting your email address anywhere on the Internet will attract spam. Share your email addresses *only* with people you know and trust.

Spammers collect email addresses using programs such as spiders, crawlers and bots that search the Internet for email addresses to add to their lists.

If you are swamped with spam, change your email address.

3. Protect yourself

Just delete it.

Don't try, don't buy and don't reply. Never visit websites or buy anything advertised in a spam message. Spam is almost always a scam. *Just delete it.*

Don't respond.

Never open, reply to or click on the "remove" or "unsubscribe" link in a spam message. These actions can confirm your email address, causing you to receive more spam.

Don't let spammers hook you like a "phish." Protect your personal information.

Spammers can reel in your valuable personal information through a practice known as "phishing." This occurs when an email shows up appearing to come from a reliable source with which you do business, like a bank or online business. Often the message suggests that there is an urgent need for you to provide personal information, such as your log-in name, passwords or even credit card numbers, often combined with the faked threat that your account will be blocked if you do not comply. In these cases, the website link provided is to a copycat, but counterfeited site. Be aware that companies will NEVER contact customers in this manner. If you have doubts, don't trust the information supplied in the email, call the company to confirm if the request is legitimate. Also, never reply to these messages or connect through the link provided in a spam that you suspect is "phishing." If you are interested in a website, access it directly through a web browser.

APPENDIX E

BACKGROUND REPORTS AND WORKING PAPERS

The following documents provide background and supplementary material on the work of the Task Force on Spam and on the conclusions of the working groups. These documents are available at **www.e-com.ic.gc.ca**.

General

- An Anti-Spam Action Plan for Canada — *Canada Gazette* Notice Summary of Submissions
- Task Force on Spam: Roundtable Meeting with Key Stakeholders
- Task Force on Spam Online Public Consultation Forum Summary of Contributions

Working Group Documents

- Anti-Spam Technology Overview
- Canadian Spam Database Concept Document
- Companion Document to *Recommended Best Practices for Internet Service Providers and Other Network Operators*
- Working Group on Legislation and Enforcement Conclusions

Background Papers

- A Statutory Private Right of Action Against Spammers in Canada
- Assessment of Email Certification
- Overview of Wireless Spam Issues in Canada
- Proposal for the Canadian Anti-Spam Action Centre
- International Spam Measures Compared

GLOSSARY

Address harvesting
The collection of lists of email addresses by automated means from websites or other online sources.

Black list
A list of IP addresses, domains or email addresses from which email is not accepted. The most common form of black list is a Domain Name System black list (DNSBL), a list of IP addresses distributed via the Internet's DNS. Popular DNSBLs include the Spamhaus Black List (SBL), the Composite Black List (CBL) and the original DNSBL, called the Mail Abuse Prevention System (MAPS) Reverse Black List (RBL). Contrast this with "white list."

Botnet
A collection of "zombies" used to send spam or for another purpose. A single botnet often contains hundreds or thousands of computers.

Bounces
The process of rejecting the attempted delivery of an email message. Sometimes a stylized "bounce report" email message reports that a previous message couldn't be delivered.

A bounce may be a "soft bounce," in which case the sending computer can retry the delivery later, or a "hard bounce," in which case the delivery is a failure.

A soft bounce may occur because the recipient's mailbox is full, the server is overloaded or there are other temporary problems. A hard bounce most often occurs because the recipient address is invalid or the recipient host, by policy, rejects mail from that sender.

Clickstream
The series of mouse clicks and related actions that a user makes while visiting a website. For an e-commerce website, a clickstream might include browsing the catalog, putting items into a virtual shopping cart, providing payment and shipping information, and then entering the order.

Cookie
A small data file created by a web server and stored on a user's computer. Cookies are a way for websites to identify users, keep track of users' preferences and recognize users who are revisiting the website. By keeping user histories, cookies let websites tailor pages and create custom experiences for individuals. Depending on how the web server is programmed, cookies may also contain personal information, such as site passwords and account numbers.

First-party cookies are ones created by the website you are visiting. Third-party cookies are created by a website other than the one you are currently visiting, most often a third-party advertiser on that site. Third-party cookies let advertisers determine whether an individual user is visiting multiple websites that display the advertiser's ads, and are often considered a privacy risk.

Modern web browsers offer options to refuse all cookies, to refuse third-party cookies and/or to accept or refuse cookies from specified websites.

Cross-sell
To encourage a customer to buy a product or service related to one already purchased. Contrast this with "up-sell."

Denial of service attack
Often abbreviated as DoS or DOS. An attempt to keep a server or network from performing its intended function, by flooding it with unwanted traffic. For example, an attacker could send tens of thousands of email messages to a mail server to overload it and keep it from processing desired mail. Many different DOS attacks and targets are possible, including attacks on mail servers, web servers, DNS servers and network routers. Spam sent in large volume can act as a DOS attack on mail servers.

Dictionary attack
An email-address guessing technique. The attacker tries to deliver email to a large number of made-up addresses, using either words out of a dictionary or letter combinations such as **aaaa@example.ca**, **aaab@example.ca** or **zzzz@example.ca**.

DNS
Domain Name System, the system that lets users locate computers on the Internet by domain name. DNS servers maintain a database of domain names (i.e. host names) and their corresponding IP addresses. For example, if the name **www.mycompany.ca** were presented to a DNS server, the IP address 204.0.8.51 might be returned. The DNS includes several different kinds of data, such as A records for IP addresses and mail exchanges (MXs) for mail servers.

The DNS is distributed among many different servers, with most servers delegating responsibility for names to other servers. In the example above, the Internet Assigned Numbers Authority (IANA), which is responsible for the entire DNS, would delegate all of **.ca** to the Canadian Internet Registration Authority (CIRA), which, in turn, would delegate all of **.mycompany.ca** to the registrant for that name, which, in turn, would operate the DNS servers that have information for **www.mycompany.ca**.

Domain
A name used on the Internet. Domains consist of multiple sections separated by dots, such as **ic.gc.ca** or **www.mycompany.com**.

Domain keys
A technology proposal by Yahoo!® that puts a cryptographic signature on messages, which recipients can verify. This provides a way to verify both that the message was sent from the domain of its email sender and that the message was not altered during transit.

EHLO/HELO identity
The name by which a sending computer identifies itself to a receiving computer at the beginning of each SMTP transaction. The command the sending computer uses to identify itself by this name to the receiving computer is called the "EHLO" or "HELO" command.

Email address
The name by which the sender or recipient of an email is identified. Each address is of the **mailbox@dom.ain** form, where **dom.ain** is a domain name that can be looked up in the DNS, and **mailbox** is an arbitrary identifier used by the domain's management to identify a mail user.

ESP or email service provider
A company that provides email services to other businesses. ESP services include collecting and maintaining lists of email addresses, sending bulk email to the addresses on the lists, removing addresses that bounce, and dealing with complaints and abuse reports related to the mailings.

Existing business relationship

An existing business relationship exists where:

1) the recipient has purchased a product or service from an organization within the past 18 months; and
2) the recipient has not unsubscribed or opted out from commercial or promotional email messages, or otherwise terminated the relationship.

An affiliate or third party may not rely on another organization's prior business relationship in order to send commercial or promotional email messages.

Filters

Software used to separate wanted from unwanted email, based on the mail's characteristics. Filters might check for specific text strings, approximate text patterns, similarity to other messages or other criteria.

Harvesting

Shorthand for "address harvesting."

Header

In Internet email, the initial part of a message, consisting of a series of lines that describe the message. Each header-line starts with a label such as From: or Subject: to identify its meaning. The header is followed by a blank line, and then the body of the message.

HTML

Hypertext markup language, the coding scheme used to format web pages and formatted email messages. HTML uses textual tags, such as <h2>A Topic</h2> to indicate a second-level header, or important text to indicate bold-faced text.

Identity theft

The use of stolen personal information to impersonate someone, generally for financial fraud purposes. An identity theft may involve impersonating a victim to gain access to existing bank accounts or take out bank loans, or for other fraudulent purposes.

IM or instant messaging

Text messages delivered immediately from the sender's computer to recipients. Popular IM systems include AOL® Instant Messenger™, Yahoo!® Messenger and MSN® Messenger.

Implied consent

The Canadian Standards Association Model Code says that "Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual." This covers situations where intended use or disclosure is obvious from the context, and the organization can assume, with little or no risk, that the individual, by providing personal information, is aware of and consents to its intended use or disclosure. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

IP address

Internet protocol address, the number that identifies a computer or other device attached to the Internet. An IP address is usually written as four decimal numbers separated by dots, as in 168.0.1.10.

Malware

A general term for hostile software such as viruses, worms and Trojan Horses.

Marketing email

Email primarily advertising the availability of goods or services. Contrast this with "transactional email."

Opt-in
Also called "express" or "positive consent." Under this form of consent, commonly referred to as "express consent," the organization presents an opportunity for the individual to express positive agreement to a stated purpose. Unless the individual takes action to "opt in" to the purpose — in other words, says "yes" to it — the organization does not assume consent. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

Opt-out
Also called "negative consent." The organization presents the individual with an opportunity to express non-agreement to an identified purpose. Unless the individual takes action to "opt out" of the purpose — that is, say "no" to it — the organization assumes consent and proceeds with the purpose. The individual should be clearly informed that the failure to "opt out" means that the individual is consenting to the proposed use or disclosure of information. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

Phishing
Impersonation of a trusted person or organization in order to steal a person's personal information, generally for the purpose of "identity theft." For example, an email message may appear to be from a well-known bank asking recipients to visit a website to confirm their account details, but the website is actually controlled by a hostile party.

Port 25 blocking
Traditionally, every computer on the Internet has had the technical ability to send mail to any other computer. In practice, most ISP customers send their outgoing mail to their ISP's mail server to be forwarded along to its ultimate recipient. In recent years, the large majority of mail sent directly, rather than via the ISP, has become spam and viruses. Many ISPs now block their customers from sending mail directly, and require it be sent via ISP mail servers, where the ISP can do virus filtering and take other anti-abuse measures. Since transmission control protocol (TCP) assigns each type of service a port number, and email is sent via port 25, this is called "port 25 blocking."

Blocking port 25 for consumer dial-up and broadband customers is widely considered a best practice.

Port 587 or SUBMIT
An alternative facility many mail systems provide for users to send outgoing mail to the ISP's mail server. It requires its sending users to authenticate themselves before sending, making SUBMIT much more auditable than port 25 mail. SUBMIT is also sometimes called port 587, after the TCP port number it uses.

rDNS or reverse DNS
Reverse Domain Name System, a service that looks up IP addresses to find domain names. It performs the opposite function of the usual DNS lookup. Reverse DNS is often used to log incoming traffic by domain name for statistical and auditing purposes. It is widely considered a best practice for all mail client and server computers to have accurate rDNS.

Role account
Email accounts that must be in place and maintained by all domains with Internet connectivity, as specified in the Internet Engineering Task Force's Request for Comments (RFCs) document series. Such accounts include **postmaster@sampledomain.ca**, **abuse@sampledomain.ca** and **hostmaster@sampledomain.ca**.

Sender ID
An authentication scheme, similar to SPF, sponsored by Microsoft. See "SPF."

Server
A computer that provides one or more services to other computers, such as email, DNS or World Wide Web pages.

SMTP
Simple Mail Transfer Protocol, the scheme used to send mail from one computer to another over the Internet. SMTP is defined in the Internet Engineering Task Force's Request for Comments series (RFC 2821).

Spam
Although there is no internationally agreed-upon definition of "spam," many countries consider it to be any bulk commercial email sent without the express consent of recipients.

SPF
Sender Policy Framework, an extension to the SMTP mail protocol on the Internet. It tries to determine the legitimacy of an email message by comparing the domain in the sender's email address to a list of computers allowed to send mail from that domain. See **http://spf.pobox.com** for more information.

Spoofing
Impersonating another person or organization to make it appear that an email message originated from somewhere other than its actual source.

Spyware
Software that collects information about a user without the user's knowledge or consent. Also, software that modifies the operation of a user's computer without the user's knowledge or consent. Typical kinds of spyware include keyloggers, which send a list to a third party of the keys that a user pressed, and adware, which displays to the user advertisements selected by the adware's owner.

Subject line
A line that is part of the headers at the beginning of each email message. Mail programs invariably display the subject lines when showing a list of messages. It is widely considered a best practice for the subject line to accurately describe the contents of the message.

Text messaging
Short messages consisting of text rather than images. Text messages can be either "instant messages" or short mobile-phone messages.

Transactional email
Email primarily containing information about current or prior business dealings, such as confirmation of a sale, a registration number, an invoice, or an opt-in or opt-out confirmation. Contrast this with "marketing email."

Transient failure
A brief malfunction that often occurs at irregular and unpredictable times.

Trojan Horse
Software that, in addition to its nominal function, secretly performs a second function.

Up-sell
To try to sell a customer a more expensive item or a more expensive version of a product or service. Contrast this with "cross-sell."

URL
Uniform resource locator, a name used to identify a web page or other online resource, typically of the form **http://www.mydomain.ca/somepage**.

Virus
"Malware" that spreads by attaching itself to another resource on a computer. Early viruses spread by attaching themselves to application programs, but current viruses spread by email. Contrast this with "worm."

Web bug
Also called a web beacon, pixel tag, clear GIF (graphics interchange format) or invisible GIF. A way for an HTML email message's sender to determine if and when the message was opened and read.

West African, 419 or Nigerian scam
An advance-fee fraud in which the perpetrator claims to be an official, typically in West Africa, who wants the victim's help to steal large amounts of money from a government account. Also known as 419 fraud, after the section number of Nigerian law that forbids it.

Before this scam moved to Africa, it was best known as the Spanish Prisoner, in which form it dates from the 1600s.

White list
A list of email addresses or IP addresses from which a mail server is configured to accept incoming mail. White lists can be useful as one part of an email filtering system. Compare this with "black list."

WHOIS
An Internet service used to ask registrars for a domain or network's registration information. It has not been universally implemented.

Worm
"Malware" that spreads directly by copying itself onto other computers through security holes in the other computers' software. The earliest worm used a security flaw in Sun Microsystems' Solaris systems and in VAX systems, but current worms all use flaws in Microsoft Windows. Contrast this with "virus."

Zombie
A computer infected by "malware" so that the computer can be remotely controlled by the creator, distributor or controller of the malware. The majority of spam is currently sent through zombies.

NOTES

FREINONS LE POURRIEL

ARRÊTEZ LE POURRIEL ICI

CRÉER UN INTERNET PLUS FORT ET PLUS SÉCURITAIRE

Rapport du Groupe de travail sur le pourriel
Mai 2005

Canada

FREINONS LE POURRIEL

ARRÊTEZ LE POURRIEL ICI

CRÉER UN INTERNET PLUS FORT ET PLUS SÉCURITAIRE

Rapport du Groupe de travail sur le pourriel
Mai 2005

On peut obtenir cette publication sur supports multiples, sur demande. Communiquer avec le Centre de diffusion de l'information dont les coordonnées suivent.

Pour obtenir des exemplaires supplémentaires de cette publication, s'adresser également au :

Centre de diffusion de l'information
Direction générale des communications et du marketing
Industrie Canada
Bureau 268D, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466
Télécopieur : (613) 954-6436
Courriel : **publications@ic.gc.ca**

Cette publication est également offerte par voie électronique sur le Web (**www.e-com.ic.gc.ca**).

Autorisation de reproduction
À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission d'Industrie Canada, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, qu'Industrie Canada soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec Industrie Canada ou avec son consentement.

Les opinions et déclarations contenues dans cette publication n'engagent que leur auteur et ne reflètent pas nécessairement la politique d'Industrie Canada ou celle du gouvernement du Canada.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, faire parvenir un courriel à **copyright.droitdauteur@tpsgc.gc.ca**.

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

N° de catalogue Iu64-24/2005
ISBN 0-662-68997-6
514279B

IMPRIMÉ AU CANADA
PRINTED IN CANADA

Couverture : 10 %
Pages intérieures : 10 %

Mai 2005

L'honorable David L. Emerson, C. P., député
Ministre de l'Industrie
Édifice C. D. Howe
tour Ouest, 5e étage
235, rue Queen
Ottawa (Ontario) K1A 0H5

Monsieur le Ministre,

Le 11 mai 2004, le gouvernement du Canada a annoncé le lancement du *Plan d'action anti-pourriel pour le Canada* et a mis sur pied un groupe de travail mixte des secteurs public et privé pour coordonner la mise en œuvre de ce plan. Nous disposions d'un an pour ce faire. Après cette période, nous devions faire rapport des progrès accomplis et proposer toute autre mesure qui pourrait s'avérer nécessaire.

Nous sommes heureux de vous informer que nous avons fait d'importants progrès dans la lutte contre le pourriel, progrès rendus possibles grâce à l'assistance de nombreuses personnes représentant tous les groupes d'intervenants qui ont contribué à nos travaux.

Nous comptions 10 membres lors de notre première réunion de comité, dans un bureau d'Ottawa, mais nous avons grandi rapidement pour former un réseau à l'échelle du pays et même au-delà. Nous avons accompli la majeure partie de notre travail en ligne, par courrier électronique. L'expérience nous a fait comprendre à quel point Internet peut transformer la façon dont nous faisons les choses et nous a convaincus de l'importance de mettre un frein au pourriel et aux autres menaces à l'utilisation d'Internet.

Notre mandat est terminé, mais il reste encore beaucoup à faire. En effet, notre expérience nous a appris que le pourriel n'est pas la seule menace à la sécurité de la plate-forme de communication et de commerce qu'est le réseau Internet. Nous avons donc recommandé une série de mesures qui contribueront à lutter contre le pourriel et les problèmes qui s'y rattachent, au Canada. Ces mesures mettront notre pays à l'avant-garde de la lutte contre un problème croissant et mondial. Nous sommes persuadés que le Canada ne doit viser rien de moins, étant donné le rôle de chef de file qu'il occupe depuis longtemps dans le domaine des communications.

Nous vous prions d'agréer, Monsieur le Ministre, l'assurance de notre très haute considération.

Lori Assheton-Smith

Michael Binder (président)

Tom Copeland

Bernard Courtois

Michael Geist

Amanda Maltby

Suzanne Morin

Geneviève Reed

Neil Schwartzman

Roger Tassé

TABLE DES MATIÈRES

Lettre de présentation iii

Sommaire 1

Recommandations 3

1. Freiner le pourriel 7
2. Clarifier les règles 11
3. Gérer les réseaux pour contrer le pourriel 18
4. Rétablir la confiance à l'égard du courriel 22
5. Sensibilisation du public 26
6. Résoudre un problème mondial 29
7. Coordonner l'action future 32

Appendices

A. Membres des sous-groupes du Groupe de travail et secrétariat 35

B. Pratiques exemplaires recommandées pour les fournisseurs de service Internet et les autres exploitants de réseaux 39

C. Pratiques exemplaires recommandées pour le marketing par courriel 45

D. Trois conseils importants pour lutter contre le pourriel 52

E. Rapports complémentaires et documents de travail 55

Glossaire 57

SOMMAIRE

QU'EST-CE QUE LE POURRIEL ET POURQUOI POSE-T-IL UN PROBLÈME?

Le *Plan d'action anti-pourriel pour le Canada* de mai 2004 définissait le pourriel comme étant « des messages électroniques commerciaux non sollicités ». Utilisant cette définition, le cabinet MessageLabs a estimé que le pourriel représentait 80 p. 100 du courriel global à la fin de 2004, comparativement à environ 10 p. 100 en 2000.

Le pourriel est plus qu'un ennui croissant. Il s'agit d'une question d'intérêt public qui pose aux gouvernements, aux fournisseurs de service Internet (FSI), aux autres exploitants de réseaux, aux expéditeurs de courriels commerciaux et aux consommateurs, le défi de collaborer d'une façon nouvelle à la solution d'un problème qui menace les intérêts de tous.

Sur une grande échelle, le pourriel menace directement la viabilité d'Internet comme moyen efficace de communication. À cause de cela, il est aussi une menace directe à la croissance de la prospérité économique, à l'efficience des services publics et au développement d'une cyberéconomie qui englobe tous les Canadiens.

Sur une petite échelle, le pourriel agace et offense les internautes. Il constitue également un véhicule pour des activités qui sont clairement illicites ou devraient l'être. Celles-ci comprennent :

- les activités nuisibles qui endommagent les ordinateurs, les réseaux ou les données, ou qui utilisent des biens personnels à des fins non autorisées (par exemple virus, vers, chevaux de Troie, attaques par déni de service, réseaux zombies);
- les pratiques commerciales trompeuses et frauduleuses, y compris les versions électroniques de fraudes postales classiques (par exemple le compte bancaire du Nigeria ou arnaque 419 et les sites Web qui personnifient des entreprises légitimes);
- les courriels hameçons visant l'usurpation d'identité ou le vol de sommes d'argent;
- les atteintes à la vie privée (par exemple collecte d'adresses électroniques, logiciels espions).

Qui le pourriel affecte-t-il?

Les menaces mentionnées minent la confiance des consommateurs à l'égard du cybercommerce et entravent les transactions électroniques entre les citoyens et leurs gouvernements. Le pourriel occasionne également des coûts importants pour l'ensemble de l'économie.

Ces coûts frappent un vaste éventail d'acteurs, notamment :

- les FSI et autres exploitants de réseaux (par exemple les grandes entreprises, les universités et les ministères gouvernementaux), qui doivent affecter des ressources techniques, financières et humaines au déploiement de technologies anti-pourriel au lieu d'investir dans des services nouveaux ou améliorés, en plus de consacrer des ressources au traitement des plaintes des clients;

- les expéditeurs de courriels commerciaux légitimes et autres utilisateurs des services de courriel, dont les messages sont filtrés par les technologies anti-pourriel avant d'atteindre leurs destinataires;
- les organismes des secteurs privé et public, dont les employés perdent du temps à s'occuper du pourriel envoyé à leur adresse de courriel professionnelle.

Au bout du compte, ces coûts frappent directement ou indirectement les consommateurs et utilisateurs finaux d'Internet. En effet, la lutte anti-pourriel occasionne des frais d'achat de logiciels de protection, empêche les améliorations de service et fait augmenter le prix des produits achetés en direct.

Que devons-nous faire pour lutter contre le pourriel?

Pour lutter contre le pourriel, le Canada doit adopter une stratégie multiple qui engage tous les intervenants. Le *Plan d'action anti-pourriel pour le Canada* de mai 2004 fut un bon départ. Il a déterminé les outils principaux pour freiner le pourriel. Ce sont :

- l'application vigoureuse des lois existantes qui interdisent le pollupostage et l'adoption d'une nouvelle loi pour combler les lacunes des lois actuelles;
- des amendes et mécanismes d'application de la loi plus puissants pour décourager les polluposteurs plus efficacement;
- des normes industrielles et des pratiques recommandées pour aider les FSI, les autres exploitants de réseaux et les entreprises de marketing par courriel dans la conduite légitime de leurs activités;
- l'éducation et la sensibilisation du public;
- la coopération internationale dans la lutte contre le pourriel.

L'année passée, le Groupe de travail sur le pourriel a dirigé l'élaboration d'une approche canadienne unique à l'égard de la lutte anti-pourriel, avec l'aide de centaines de personnes représentant différents groupes d'intervenants. Le présent rapport décrit ses activités ainsi que le travail qui reste à faire. Au cours de ses travaux, le Groupe de travail a retenu plusieurs leçons d'importance dans la lutte anti-pourriel, non seulement au Canada mais également dans le monde.

L'importance d'une démarche multiple, regroupant divers intervenants

La leçon la plus importante est la suivante : une démarche anti-pourriel multiple, regroupant divers intervenants, fonctionne, et c'est sans doute la seule qui sera efficace à long terme.

Certains pays ont choisi de combattre le pourriel principalement à l'aide de lois et de règlements. Les travaux du Groupe de travail ont confirmé qu'il fallait mettre en œuvre des lois claires et des sanctions sévères et les appliquer rigoureusement pour lutter de façon efficace contre le pourriel. Ils ont également démontré l'importance de combler les lacunes de la législation canadienne actuelle et de corriger les faiblesses du système d'application de la loi. Mais, malgré leur importance, les démarches juridiques à elles seules ne garantiront pas la victoire.

Des pratiques commerciales solides, la sensibilisation des consommateurs, l'éducation du public et la collaboration internationale sont des composantes tout aussi importantes de l'approche de type « boîte à outils » pour combattre le pourriel. Pour obtenir les meilleurs résultats possibles, on doit élaborer et utiliser ces outils d'une façon coordonnée, au sein d'un cadre juridique solide renforcé par un système d'application efficace.

L'importance de la communication et de la coopération entre intervenants

La deuxième leçon retenue est la suivante : les différents groupes d'intervenants concernés par la lutte anti-pourriel doivent communiquer et travailler ensemble.

Lorsqu'il a entamé ses travaux, le Groupe de travail a rapidement découvert que la structure du groupe des intervenants était cloisonnée et qu'il se devait de combler l'écart pouvant exister normalement entre le gouvernement, le secteur privé et les défenseurs de l'intérêt public, écart dû aux intérêts et aux points de vue divergents.

Les travaux pratiques effectués en commun se sont avérés un moyen très efficace d'éliminer ces obstacles. En plus d'améliorer les communications, la démarche multilatérale adoptée par le Groupe de travail a produit des résultats très significatifs

en ce qui concerne la création de précédents liés à l'établissement de mesures d'application de la loi anti-pourriel, de pratiques exemplaires à l'avant-garde mondiale pour le secteur industriel ainsi que de campagnes de sensibilisation et d'éducation du public fort efficaces.

L'obtention de résultats pratiques dans la lutte anti-pourriel exigera une coordination continue des travaux des intervenants au moyen de bonnes communications.

L'importance d'une stratégie globale dans la lutte contre les menaces à Internet

La troisième leçon retenue est la suivante : la lutte anti-pourriel n'est qu'un élément d'un combat beaucoup plus vaste qui s'engage contre les dangers nouveaux et potentiellement plus sérieux qui menacent Internet en matière de communications et de commerce.

Lorsque le Canada a commencé l'élaboration du *Plan d'action anti-pourriel pour le Canada*, il y a deux ou trois ans, le pourriel était considéré comme un ennui qui occasionnait des pertes de temps aux consommateurs et aux entreprises. C'était encore l'opinion générale qui existait au moment où le Groupe de travail a entamé ses travaux.

Durant l'année passée, le Groupe de travail s'est rendu compte que le pourriel était devenu plus qu'un ennui mineur. Le pourriel est une source croissante d'activités visant à tromper, à enfreindre la vie privée, à faire un usage non autorisé du matériel des consommateurs et des entreprises, à endommager les ordinateurs et les réseaux, à commettre de la fraude et à voler des renseignements personnels.

Pendant cette même période, le pourriel et les autres genres de menaces ont commencé à se propager du courriel à la messagerie instantanée et aux communications sans fil.

C'est pourquoi, en préparant le rapport, le Groupe de travail a tenté d'aller au-delà du problème familier du courriel commercial non sollicité et d'effectuer une analyse exhaustive et stratégique des défis que le Canada devra relever pour venir à bout du pourriel et des autres menaces à Internet.

Recommandations

Pour lutter contre le pourriel, le Groupe de travail recommande les démarches suivantes :

Leadership et partenariat

1. Le gouvernement fédéral, en association avec d'autres intervenants, devrait continuer à préconiser une stratégie à facettes multiples pour mettre fin au pourriel.

Législation, réglementation et application de la loi

2. Le gouvernement fédéral devrait adopter un ensemble de règlements judiciaires précis, visant à interdire le pourriel et les nouvelles menaces à la sécurité du réseau Internet (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) et, pour ce faire, adopter une nouvelle loi et modifier les lois actuelles au besoin.
3. À cette fin, les activités et pratiques de multi-postage abusif suivantes devraient constituer des infractions au titre d'une loi anti-pourriel spécifique (ces dispositions peuvent également être énoncées, en totalité ou en partie, dans les lois actuelles) :
   - le défaut de se conformer à des procédures d'inclusion pour l'envoi de courriels non sollicités;
   - l'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, le but ou le contenu d'un courriel, que l'objectif soit de tromper le destinataire ou de contourner les filtres techniques;
   - la construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées);
   - la collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes;
   - les attaques de dictionnaire.

4. Les sanctions et recours suivants devraient s'appliquer à ces nouvelles infractions :

   - les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions énumérées à la recommandation 3;
   - un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile;
   - les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient aussi être tenues responsables du pourriel. La responsabilité devrait également incomber aux tiers qui bénéficient du pourriel.

5. En ce qui concerne l'application et l'administration de la nouvelle loi :

   - l'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public, et l'octroi d'un soutien aux organismes d'application;
   - l'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.

6. Le gouvernement fédéral devrait accorder la priorité à l'application des mesures anti-pourriel en renforçant le soutien et les ressources destinés aux organismes responsables de l'application des lois anti-pourriel nouvelles et actuelles.

7. Le gouvernement fédéral, de concert avec les provinces et les territoires, devrait conclure et mettre en œuvre des accords de coopération en matière d'application des lois avec d'autres pays. Toutes les dispositions législatives actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre d'enquêtes coopératives et de mesures de mise en application homogènes, à l'échelle internationale.

Pratiques exemplaires pour les fournisseurs de service Internet et les autres exploitants de réseaux

8. Les FSI et autres exploitants de réseaux devraient mettent en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel.

9. Les FSI et autres exploitants de réseaux, en coopération avec l'organisme de coordination établi par le ministre de l'Industrie (mentionné à la recommandation 5), devraient mesurer de façon continue l'ampleur du problème du pourriel au Canada et évaluer les répercussions des pratiques recommandées. Ils devraient continuer à cerner les questions qui pourraient mériter davantage d'examen et mener à la formulation de recommandations additionnelles.

10. Afin de faciliter de façon continue la surveillance des tendances du pourriel et l'élaboration de mesures et de techniques anti-pourriel, le gouvernement devrait jouer un rôle de leadership en créant une base de données canadienne sur les pourriels (« congélateur à pourriels »).

11. Les FSI et autres exploitants de réseaux devraient adopter et appliquer des Politiques d'utilisation acceptable interdisant clairement le pollupostage sur leurs réseaux.

Pratiques exemplaires pour le marketing par courriel

12. Les entreprises de marketing par courriel devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel et, de concert avec l'organisme de coordination mis sur pied par le ministre de l'Industrie, devraient évaluer continuellement l'efficacité de ces pratiques.

13. Le secteur industriel canadien, en coordination avec les organismes internationaux d'élaboration de normes, devrait continuer d'étudier diverses méthodes de certification et leurs frais connexes pour déterminer quelle méthode, s'il en est, constituerait le régime de certification le plus approprié au Canada.

14. Pour déterminer la portée du problème de non-livraison du courriel légitime au Canada, l'organisme de coordination mis sur pied par le ministre de l'Industrie devrait étudier officiellement cette question de façon permanente, avec l'aide des intervenants appropriés.

Sensibilisation et éducation des utilisateurs

15. Dans le cadre des efforts continus qu'il déploie pour accroître la sensibilisation et l'éducation des utilisateurs, le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de promouvoir la campagne axée sur les conseils aux utilisateurs « Arrêtez le pourriel ici / Stop Spam Here », en encourageant les responsables d'autres sites Web à placer dans leur site un lien qui y donne accès et en utilisant d'autres méthodes et médias appropriés.

16. Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de maintenir et d'enrichir les deux versions du site Web « Arrêtez le pourriel ici / Stop Spam Here ». Le but est d'en faire un mécanisme plus efficace comme outil d'éducation et source de liens utiles donnant accès à d'autres ressources de lutte contre le pourriel, et de veiller à ce que les deux versions demeurent à jour et pertinentes (par exemple, en y affichant de l'information sur les pratiques exemplaires du secteur industriel, la future législation anti-pourriel et les procédures à suivre pour déposer une plainte).

17. Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait élaborer des campagnes de sensibilisation et d'éducation efficaces et cohérentes adaptées aux besoins de différents groupes de destinataires cibles en matière de lutte contre le pourriel.

Collaboration internationale

18. Le gouvernement fédéral devrait continuer de conclure avec des gouvernements étrangers des accords bilatéraux sur les politiques et les stratégies anti-pourriel.

19. Le gouvernement fédéral, en consultation, en collaboration et en partenariat avec d'autres intervenants s'il y a lieu, devrait promouvoir et appuyer de façon active la mise en œuvre coordonnée au niveau international des mesures politiques, législatives, réglementaires et d'application, des normes et pratiques du secteur industriel et des activités d'éducation et de sensibilisation du public dans le domaine de la lutte contre le pourriel.

20. Le Canada devrait mettre au service des pays en développement ses compétences dans l'élaboration d'approches multiples, de type boîte à outils, et mettant à contribution différents intervenants, pour les aider à lutter contre le pourriel.

Mise sur pied d'un organisme de coordination

21. Afin de poursuivre la démarche multiple, de type « boîte à outils » et regroupant divers intervenants formulée par le Groupe de travail sur le pourriel et de fournir un point central pour faciliter la mise en œuvre de ses recommandations, le gouvernement devrait établir un centre relevant du ministre de l'Industrie, qui assumerait la supervision et la coordination des politiques, l'éducation et la sensibilisation du public et fournirait un appui aux organismes d'application des lois.

22. Le gouvernement fédéral, par le truchement de cet organisme de coordination, devrait surveiller les répercussions de la mise en œuvre des recommandations du Groupe de travail, évaluer les résultats, faire rapport régulièrement au public et, en consultation avec les intervenants, prendre toutes les mesures supplémentaires requises pour lutter contre le pourriel.

1 FREINER LE POURRIEL

QU'EST-CE QUE LE POURRIEL ET POURQUOI POSE-T-IL UN PROBLÈME?

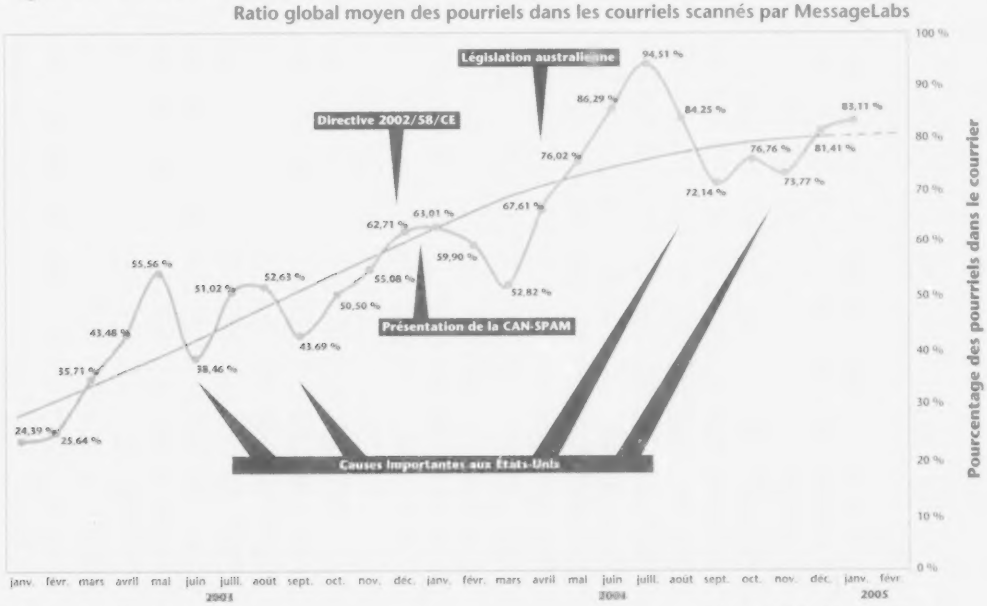
En quelques années seulement, le volume de messages électroniques commerciaux non sollicités, communément appelés « pourriels », est devenu, de l'ennui mineur qu'il était, un problème social et économique important qui mine la productivité individuelle et commerciale des Canadiens, ainsi qu'une couverture aux activités criminelles. Le pourriel entrave l'utilisation efficace du courriel pour les communications personnelles et commerciales, et menace la croissance et l'acceptation du commerce électronique légitime.

Les rapports sur la circulation du courriel indiquent que le pourriel représentait environ 10 p. 100 du volume total de courriels en 2000. Comme l'illustre la figure 1 :

- à la fin de 2002, il en représentait 30 p. 100;
- au milieu de 2003, le nombre de messages électroniques commerciaux non sollicités avait dépassé celui des communications légitimes;
- à la fin de 2004, le pourriel représentait 80 p. 100 du courriel global.

Figure 1 — Tendances globales du pourriel, 2003-2005

Ratio global moyen des pourriels dans les courriels scannés par MessageLabs



Source : www.messagelabs.com (traduction)

MessageLabs Ltd., Tous droits réservés, 2005

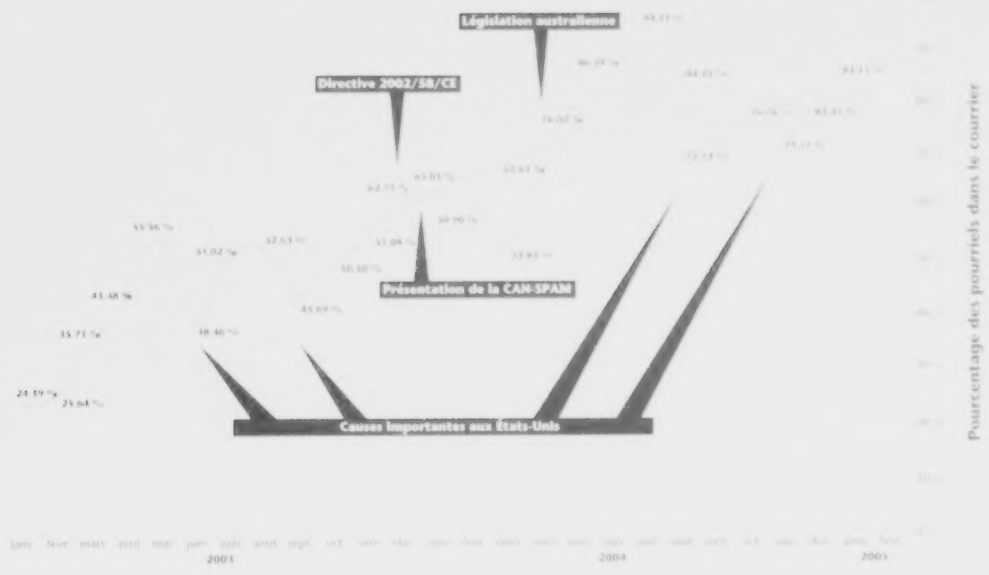
1 FREINER LE POURRIEL

En quelques années seulement, le volume de messages électroniques commerciaux non sollicités, communément appelés « pourriels », est devenu, de l'ennui mineur qu'il était, un problème social et économique important qui mine la productivité individuelle et commerciale des Canadiens, ainsi qu'une couverture aux activités criminelles. Le pourriel entrave l'utilisation efficace du courriel pour les communications personnelles et commerciales, et menace la croissance et l'acceptation du commerce électronique légitime.

Les rapports sur la circulation du courriel indiquent que le pourriel représentait environ 10 p. 100 du volume total de courriels en 2000. Comme l'illustre la figure 1

- à la fin de 2002, il en représentait 30 p. 100;
- au milieu de 2003, le nombre de messages électroniques commerciaux non sollicités avait dépassé celui des communications légitimes;
- à la fin de 2004, le pourriel représentait 80 p. 100 du courriel global.

Ratio global moyen des pourriels dans les courriels scannés par MessageLabs



Il est maintenant reconnu que le volume croissant du pourriel a une influence sur le prix demandé par les entreprises qui fournissent des services Internet. Ce coût est au bout du compte assumé par les organismes et les entreprises qui utilisent les communications électroniques pour leurs affaires, et il est reflété dans les frais de service des particuliers qui utilisent Internet afin de communiquer avec leur famille, leurs amis et d'autres correspondants.

La nature de la menace posée par le pourriel évolue à mesure que le volume global de pourriels augmente. Il est vrai que les techniques de filtrage améliorées et autres mesures de protection adoptées par les FSI et les consommateurs ont contribué à réduire le nombre de pourriels qui entrent dans les boîtes aux lettres des internautes. D'ailleurs, un sondage d'opinion publique publié dans le *Canadian Inter@ctive Reid Report* d'Ipsos-Reid pour le quatrième trimestre de 2004, rapporte que les Canadiens croient recevoir moins de pourriel qu'il y a un an. Néanmoins, la tendance persistante à la hausse, illustrée dans la figure 1, demeure un problème important pour les FSI et les utilisateurs qui doivent assumer le fardeau des coûts associés au filtrage ou à l'élimination du pourriel.

Une tendance est cependant encore plus importante. On constate que, même si le volume de pourriels traditionnels diminuait, les menaces posées par les nouvelles formes de pourriel augmenteraient. Ces menaces plus vastes à la sécurité d'Internet incluent entre autres les logiciels espions, les virus, l'hameçonnage et les réseaux d'ordinateurs zombies. Des rapports récents démontrent que ces menaces ont considérablement augmenté depuis le début des travaux du Groupe de travail il y a un an. Par exemple :

- MessageLabs a fait rapport de 18 millions de courriels hameçons en 2004.
- L'étude *Online Safety Study* d'AOL®—National Cyber Security Alliance, publiée en octobre 2004, rapporte que 80 p. 100 des utilisateurs américains ont des logiciels espions ou publicitaires sur leurs ordinateurs et que 89 p. 100 d'entre eux en ignorent la présence.

Les récentes formes de pourriel minent la confiance des consommateurs à l'égard d'Internet en tant que plate-forme de commerce électronique et de communication. À cause de cela, la capacité des technologies de l'information et des communications d'appuyer la productivité, et celle du commerce électronique d'attirer l'investissement, de créer des emplois et d'enrichir nos vies, sont entravées par le poids des pourriels et des activités trompeuses, frauduleuses et nuisibles qui l'accompagnent parfois.

Principes directeurs du Plan d'action anti-pourriel pour le Canada

L'ampleur des préoccupations suscitées au sein du grand public et le coût croissant que doit subir notre économie indiquent clairement qu'il est temps que les pouvoirs publics, le milieu des affaires, le secteur du marketing et les consommateurs fassent front commun afin de réduire et de contrôler les pourriels.

Il est évident que le pourriel est un problème multiple qui demande que l'on prenne des mesures concertées à plusieurs niveaux, afin d'arriver à des résultats réels et mesurables. Intervenants canadiens et partenaires internationaux s'entendent sur les principes suivants :

- Les courriels commerciaux envoyés avec le consentement préalable et continu du destinataire ne sont pas des pourriels et occupent une place légitime dans le commerce électronique.
- Les courriels commerciaux envoyés sans consentement préalable, ou qui sont trompeurs, frauduleux ou nuisibles, sont des pourriels et doivent être interdits.
- Le recours aux lois actuelles et à d'éventuelles nouvelles lois pour lutter contre le pourriel mérite d'être examiné. Toutefois, à moins que les organismes d'application de la loi accordent une grande priorité et suffisamment de ressources aux actions anti-pourriel, les lois à elles seules n'endigueront pas la circulation des pourriels, ni les menaces connexes, même si ces lois sont assorties de mesures techniques, de meilleures pratiques commerciales et d'un changement de comportement de la part des consommateurs.

- On s'entend pour affirmer que le gouvernement devrait éviter de prescrire des solutions techniques détaillées. Au lieu de cela, il devrait encourager et aider tous ses partenaires à utiliser et à partager les meilleures solutions techniques et pratiques commerciales et de consommation.
- Une solution efficace au problème du pourriel exige non seulement une action concertée de la part de tous les partenaires canadiens, mais également une collaboration accrue à l'échelle internationale. Bien que, malheureusement, le Canada demeure une source de pourriel, la majorité des pourriels reçus par des Canadiens émane de l'étranger. Une démarche anti-pourriel internationale efficace nécessitera une action concertée de la part des gouvernements et autres intervenants.

Mandat, structure et méthodes de travail du Groupe de travail sur le pourriel

Le 11 mai 2004, la ministre de l'Industrie a annoncé le lancement du *Plan d'action anti-pourriel pour le Canada* visant à réduire le volume des courriels commerciaux non sollicités et a mis sur pied le Groupe de travail sur le pourriel afin de coordonner la mise en œuvre du Plan d'action. Présidé par Industrie Canada, le Groupe de travail réunit des experts et des intervenants clés représentant les FSI, les entreprises canadiennes qui utilisent le courriel à des fins commerciales légitimes et les consommateurs.

Le Groupe de travail disposait d'un an pour voir à la mise en œuvre du Plan d'action et la coordonner. Après cette période, il devait faire rapport sur les progrès accomplis et proposer toute autre initiative pouvant s'avérer nécessaire, y compris des mesures législatives.

Malgré le nombre réduit de ses membres, le Groupe de travail représentait un vaste éventail d'organisations qui s'intéressaient à l'avenir des communications par courriel, allant des utilisateurs individuels aux grands concepteurs et fournisseurs des logiciels et du matériel qui alimentent la croissance d'Internet. Afin d'organiser ses travaux et de recruter d'autres intervenants, le Groupe de travail a mis sur pied cinq sous-groupes pour traiter des points précis abordés dans le Plan d'action :

- la législation et son application
- les technologies et la gestion de réseaux
- la validation du courriel commercial
- l'éducation et la sensibilisation du public
- la collaboration internationale

La participation aux groupes de travail était ouverte à toute personne ou organisation intéressée. Environ 60 organisations ont répondu à l'appel (voir la liste à l'appendice A).

On a demandé au Groupe de travail, durant son mandat, de réunir les principaux intervenants afin d'examiner la mise en œuvre du Plan d'action et de cerner d'autres domaines susceptibles d'exiger une nouvelle initiative. Pour ce faire, il a organisé une table ronde des intervenants le 3 décembre 2004.

On a également demandé au Groupe de travail de consulter tous les intervenants et les Canadiens intéressés à exprimer leur opinion ou à contribuer à ses travaux. À cette fin, il a publié un avis dans la *Gazette du Canada* durant l'été 2004 et a établi un forum en ligne où les particuliers pouvaient exprimer leur opinion sur n'importe quel sujet étudié par le Groupe de travail.

Recommandation générale

L'expérience du Groupe de travail a démontré l'importance et la nécessité d'avoir recours à une approche multiple pour lutter contre le pourriel. Bien que la lutte contre les courriels commerciaux non sollicités ait considérablement progressé pendant l'année qui vient de s'écouler, il reste encore beaucoup à faire.

De plus, l'apparition de nouvelles menaces bien plus graves à la sécurité d'Internet, tels les logiciels espions et l'usurpation d'identité découlant du hameçonnage et autres activités illicites en ligne, souligne l'importance de conserver l'élan des différents intervenants, dans la foulée des travaux du Groupe de travail.

Le Groupe de travail a conclu que la réussite de la lutte anti-pourriel exigeait l'établissement d'un organisme central chargé de coordonner les démarches visant à contrer le pourriel et les activités illicites connexes.

C'est pourquoi nous formulons la recommandation suivante :

Recommandation 1 :

Le gouvernement fédéral, en association avec d'autres intervenants, devrait continuer à préconiser une stratégie à facettes multiples pour mettre fin au pourriel.

2 CLARIFIER LES RÈGLES

LE DÉFI

Les marchés traditionnels des biens et services sont régis par des lois et des règlements destinés à promouvoir la concurrence loyale et à protéger les consommateurs. Pour fonctionner efficacement, le cybercommerce requiert des règlements semblables pour guider le comportement commercial. Tel que discuté dans le chapitre précédent, le pourriel pose une menace de taille au développement du cybercommerce, car il occasionne des coûts, crée de l'inefficacité, cause du tort et entrave la confiance des entreprises et des consommateurs.

Des mesures telles que le renforcement des lois actuelles, la sensibilisation des entreprises et des consommateurs et la promotion de l'éducation du public permettraient d'éliminer certaines menaces attribuables au pourriel. Toutefois, il est peu probable que ces mesures viennent à bout des polluposteurs vraiment malhonnêtes — ceux qui entendent commettre une fraude, usurper l'identité ou enfreindre la vie privée des gens, obtenir un accès non autorisé ou endommager les ordinateurs et le matériel de réseau. Il faut donc mettre en œuvre des lois plus précises interdisant le comportement illicite, prévoir des peines sévères et appliquer rigoureusement les lois pour traiter ce genre de menace et appuyer la démarche anti-pourriel de type « boîte à outils » du Canada.

La mise en œuvre d'un cadre national solide sera encore plus essentielle, à mesure que le pourriel deviendra de plus en plus le véhicule d'activités telles que l'hameçonnage et de technologies comme les logiciels espions, les virus et les réseaux d'ordinateurs zombies, qui, en minant la confiance, menacent sérieusement l'utilisation d'Internet en tant que plate-forme pour le commerce. Internet fait maintenant partie de l'infrastructure essentielle du pays, et il faut être capable d'éliminer ces menaces à sa sécurité.

Un cadre national solide permettrait également au Canada de prendre part à la lutte internationale contre le pourriel. La grande majorité des pourriels envoyés aux citoyens et aux entreprises du Canada provient de l'étranger. Cependant, avec un cadre législatif précis et solide, ainsi que des mécanismes d'application efficaces, le Canada serait bien positionné pour contribuer à la mise au point de démarches internationales harmonisées et de mesures d'application concertées.

L'une des premières questions qui s'est posée au Groupe de travail sur le pourriel était la mesure dans laquelle le cadre juridique et les mesures d'application actuellement en vigueur au Canada pourraient servir à combattre le pourriel.

Lors de l'élaboration du *Plan d'action anti-pourriel pour le Canada*, bon nombre d'intervenants ont déclaré qu'une meilleure application des lois fédérales existantes pourrait réduire sensiblement le volume du pourriel. Ils ont cité, notamment, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la *Loi sur la concurrence* et le *Code criminel du Canada* comme étant des outils pouvant servir à la réduction du courriel commercial non sollicité. Les motifs invoqués étaient les suivants.

- La LPRPDE, conçue de manière à protéger les renseignements personnels à l'ère électronique, interdit la collecte, l'utilisation ou la divulgation des renseignements personnels d'une personne, y compris son adresse de courriel, sans son consentement. Cette loi précise également que les renseignements personnels ne peuvent être utilisés à des fins autres que celles pour lesquelles ils sont recueillis, et que les propriétaires de ces renseignements doivent consentir à toute utilisation secondaire qui en est faite. Par conséquent, tout courriel non sollicité envoyé à l'adresse de courriel d'un particulier qui n'a pas consenti à le recevoir pourrait enfreindre cette loi fédérale et, peut-être, d'autres lois provinciales essentiellement similaires.
- La *Loi sur la concurrence* renferme des dispositions formelles à l'égard des représentations déloyales et trompeuses auxquelles on a souvent recours pour traiter la publicité mensongère publiée dans les médias traditionnels. L'application de la Loi aux revendications trompeuses contenues dans les sollicitations par courriel, est un domaine digne d'examen.
- Le *Code criminel du Canada* renferme des dispositions traitant spécifiquement de l'accès non autorisé aux systèmes et aux réseaux informatiques, de l'endommagement des données, ainsi que des dispositions plus générales concernant la fraude. Vu que bon nombre de polluposteurs enchâssent dans les courriels des « chevaux de Troie » pouvant être activés par les multiposteurs pour transmettre un pourriel, on pourrait éventuellement utiliser le *Code criminel du Canada* afin de punir ces délits. Ses dispositions prévoient des amendes importantes et même des peines d'emprisonnement.

Bien que les lois actuelles comportent des dispositions potentiellement utilisables dans la lutte contre le pourriel, le Groupe de travail a noté que leur efficacité était une question discutable, étant donné que la majorité d'entre elles n'ont pas encore été appliquées à des cas de pourriels.

Le premier défi du Groupe de travail consistait donc à examiner l'application du cadre juridique et des mécanismes d'application actuels du Canada à la lutte contre le pourriel. Pour ce faire, il a décidé de travailler avec les ministères et les organismes du gouvernement à l'examen des lois et des mécanismes d'application actuels pour déterminer s'ils comportent des lacunes susceptibles de les rendre inefficaces dans la lutte anti-pourriel.

Puisque cela s'est révélé être le cas, le deuxième défi était de déterminer quelles mesures il faudrait adopter pour combler ces lacunes et doter le Canada d'un cadre juridique efficace et d'une démarche nationale concertée afin de contrer le pourriel et les activités connexes.

Activités du Groupe de travail

Sensibilisation et action catalytique des organismes d'application de la loi

La première tâche du Groupe de travail a été d'organiser des entretiens entre des sociétés privées et les organismes d'application des lois fédérales responsables de la législation susceptible d'être utilisée afin de contrer le pourriel, notamment le Bureau de la concurrence, le Commissariat à la protection de la vie privée du Canada et la Gendarmerie royale du Canada (GRC). L'objectif était d'évaluer l'efficacité de chaque loi pour les poursuites fondées sur des infractions liées au pourriel.

En première étape, le Groupe de travail a identifié toutes les lois fédérales pouvant s'appliquer aux diverses facettes du pourriel. Il a décidé de concentrer ses efforts sur les facettes ayant les liens les plus clairement associés aux lois actuelles. Le Groupe de travail a créé quelques sous-groupes pour aborder les exigences des diverses situations de fait, associées aux poursuites selon chaque loi. Au moment de la publication de ce rapport, trois plaintes ont été réglées en vertu de la LPRPDE, et une l'a été en vertu de la *Loi sur la concurrence* (voir l'encadré 1 — Récentes poursuites reliées au pourriel).

Peu de progrès ont été réalisés quant à l'application du *Code criminel du Canada*, à cause d'un manque de priorisation et de questions de compétence. En effet, les poursuites relèvent des administrations provinciales et des organismes locaux d'application de la loi. Cependant, le Groupe de travail a collaboré avec ces groupes pour faire progresser les travaux. En outre, il a travaillé avec Justice Canada et la Direction de la criminalité technologique de la GRC, afin de cerner les éléments de preuve voulus pour intenter une poursuite en vertu de dispositions précises du *Code criminel*.

Encadré 1 — Récentes poursuites reliées au pourriel

Décisions relatives à des plaintes déposées devant le Commissariat à la protection de la vie privée du Canada
Deux membres du Groupe de travail sur le pourriel ont porté plainte en vertu de la LPRPDE.

Michael Geist a reçu deux courriels l'invitant à acheter des billets de saison d'une équipe de football locale. Le bureau de l'équipe avait obtenu son adresse de courriel sur les sites Web de son université et de son cabinet juridique. M. Geist a déposé une plainte auprès du Commissariat à la protection de la vie privée, à la réception du deuxième courriel, après avoir demandé d'être rayé de la liste d'envoi.

Le commissaire à la protection de la vie privée a déterminé qu'une adresse de courriel commerciale est un renseignement personnel protégé par la LPRPDE. Ce genre de renseignement peut être recueilli et utilisé sans le consentement de la personne concernée, mais uniquement aux fins prévues (c'est-à-dire associées aux activités professionnelles de M. Geist). Le commissaire a conclu que l'équipe de football ne pouvait invoquer cette exception, étant donné que ses intentions étaient totalement étrangères aux fins pour lesquelles l'adresse de courriel avait été publiée.

Suzanne Morin a reçu des sollicitations par courriel, à son adresse de courriel commerciale, d'une société différente de celle de M. Geist. L'adresse de courriel provenait du répertoire électronique des membres d'une association professionnelle. M^me^ Morin a déposé une plainte auprès du Commissariat à la protection de la vie privée. Le commissaire a jugé, encore une fois, qu'en vertu de la LPRPDE, une adresse de courriel commerciale est un renseignement personnel. Le commissaire a déterminé que la collecte et l'utilisation subséquente de l'adresse de courriel aux fins de sollicitations commerciales avaient été effectuées par la société de marketing sans le consentement de M^me^ Morin et qu'il y avait eu violation de la Loi.

Dans les deux cas, les organismes ont présenté des excuses, retiré les adresses de courriel de leurs listes de marketing et modifié leurs procédures internes en conséquence.

Règlement d'un cas par le Bureau de la concurrence
Performance Marketing Ltd. a fait de fausses représentations selon lesquelles les timbres Zyapex et Dyapex étaient des produits naturels et sans danger qui permettaient de perdre du poids, donnant ainsi la fausse impression que, sans suivre de régime ni effectuer d'exercice physique, une personne pourrait perdre du poids, avoir moins d'appétit, contrôler son envie de manger et accélérer son métabolisme. Ces allégations ont été faites par courriel. Performance Marketing a aussi échoué à mettre en œuvre sa politique anti-pourriel, ce qui a incité ses filiales à avoir recours au pourriel pour vendre les produits.

La cause a été jugée en vertu du Projet FrancNet du Bureau de la concurrence, destiné à éliminer la publicité trompeuse qui se retrouve dans Internet. Aux termes du consentement intervenu avec Performance Marketing en décembre 2004, la société s'est engagée à veiller à ce que le pourriel ne soit pas un véhicule de commercialisation de ses produits, à afficher un avis correctif dans son site Web et à rembourser intégralement les consommateurs qui avaient acheté les timbres coupe-faim.

Suite à des entretiens avec le secteur canadien des communications sans fil, on a soulevé la possibilité d'appliquer les dispositions de la *Loi sur les télécommunications* au pourriel envoyé aux combinés sans fil. L'adoption du projet de loi C-37 (prévoyant la création d'une liste nationale de numéros de téléphone exclus) pourrait renforcer la capacité du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) de mettre un frein au pourriel acheminé par les appareils sans fil — précisément l'envoi électronique de pourriels par messagerie texte aux combinés sans fil. Le pouvoir du CRTC d'imposer des amendes revêtirait une importance particulière. Mais avant l'adoption du projet de loi C-37, il est peut-être encore trop tôt pour juger du rôle que la *Loi sur les télécommunications* pourrait jouer.

Problème de la mise en application des lois

Durant les étapes initiales de ses travaux, le Groupe de travail sur le pourriel a informé les deux organismes d'application de la loi de l'ampleur et de la gravité du problème du pourriel, et a mis les sociétés privées au fait des exigences juridiques et des critères de preuve relatifs aux poursuites. Parallèlement à ces travaux, certains organismes d'application de la loi ont entamé une action directe contre les polluposteurs (voir l'encadré 1 ci-dessus). Néanmoins, les mesures d'application ont été peu efficaces jusqu'à présent.

En effet, les organismes d'application ont de la difficulté à appliquer leur loi à toutes les facettes du pourriel. Qui plus est, les deux organismes d'application concernés, tout comme la GRC et les autorités policières locales, ont des ressources restreintes et des priorités conflictuelles qui limitent leur capacité d'intervention. L'application

Décisions relatives à des plaintes déposées devant le Commissariat à la protection de la vie privée du Canada
Deux membres du Groupe de travail sur le pourriel ont porté plainte en vertu de la LPRPDE.

Michael Geist a reçu deux courriels l'invitant à acheter des billets de saison d'une équipe de football locale. Le bureau de l'équipe avait obtenu son adresse de courriel sur les sites Web de son université et de son cabinet juridique. M. Geist a déposé une plainte auprès du Commissariat à la protection de la vie privée, à la réception du deuxième courriel, après avoir demandé d'être rayé de la liste d'envoi.

Le commissaire à la protection de la vie privée a déterminé qu'une adresse de courriel commerciale est un renseignement personnel protégé par la LPRPDE. Ce genre de renseignement peut être recueilli et utilisé sans le consentement de la personne concernée, mais uniquement aux fins prévues (c'est-à-dire associées aux activités professionnelles de M. Geist). Le commissaire a conclu que l'équipe de football ne pouvait invoquer cette exception, étant donné que ses intentions étaient totalement étrangères aux fins pour lesquelles l'adresse de courriel avait été publiée.

Suzanne Morin a reçu des sollicitations par courriel, à son adresse de courriel commerciale, d'une société différente de celle de M. Geist. L'adresse de courriel provenait du répertoire électronique des membres d'une association professionnelle. M^me^ Morin a déposé une plainte auprès du Commissariat à la protection de la vie privée. Le commissaire a jugé, encore une fois, qu'en vertu de la LPRPDE, une adresse de courriel commerciale est un renseignement personnel. Le commissaire a déterminé que la collecte et l'utilisation subséquente de l'adresse de courriel aux fins de sollicitations commerciales avaient été effectuées par la société de marketing sans le consentement de M^me^ Morin et qu'il y avait eu violation de la Loi.

Dans les deux cas, les organismes ont présenté des excuses, retiré les adresses de courriel de leurs listes de marketing et modifié leurs procédures internes en conséquence.

Règlement d'un cas par le Bureau de la concurrence
Performance Marketing Ltd. a fait de fausses représentations selon lesquelles les timbres Zyapex et Dyapex étaient des produits naturels et sans danger qui permettaient de perdre du poids, donnant ainsi la fausse impression que, sans suivre de régime ni effectuer d'exercice physique, une personne pourrait perdre du poids, avoir moins d'appétit, contrôler son envie de manger et accélérer son métabolisme. Ces allégations ont été faites par courriel. Performance Marketing a aussi échoué à mettre en œuvre sa politique anti-pourriel, ce qui a incité ses filiales à avoir recours au pourriel pour vendre les produits.

La cause a été jugée en vertu du Projet FrancNet du Bureau de la concurrence, destiné à éliminer la publicité trompeuse qui se retrouve dans Internet. Aux termes du consentement intervenu avec Performance Marketing en décembre 2004, la société s'est engagée à veiller à ce que le pourriel ne soit pas un véhicule de commercialisation de ses produits, à afficher un avis correctif dans son site Web et à rembourser intégralement les consommateurs qui avaient acheté les timbres coupe-faim.

Suite à des entretiens avec le secteur canadien des communications sans fil, on a soulevé la possibilité d'appliquer les dispositions de la *Loi sur les télécommunications* au pourriel envoyé aux combinés sans fil. L'adoption du projet de loi C-37 (prévoyant la création d'une liste nationale de numéros de téléphone exclus) pourrait renforcer la capacité du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) de mettre un frein au pourriel acheminé par les appareils sans fil — précisément l'envoi électronique de pourriels par messagerie texte aux combinés sans fil. Le pouvoir du CRTC d'imposer des amendes revêtirait une importance particulière. Mais avant l'adoption du projet de loi C-37, il est peut-être encore trop tôt pour juger du rôle que la *Loi sur les télécommunications* pourrait jouer.

Durant les étapes initiales de ses travaux, le Groupe de travail sur le pourriel a informé les deux organismes d'application de la loi de l'ampleur et de la gravité du problème du pourriel, et a mis les sociétés privées au fait des exigences juridiques et des critères de preuve relatifs aux poursuites. Parallèlement à ces travaux, certains organismes d'application de la loi ont entamé une action directe contre les polluposteurs (voir l'encadré 1 ci-dessus). Néanmoins, les mesures d'application ont été peu efficaces jusqu'à présent.

En effet, les organismes d'application ont de la difficulté à appliquer leur loi à toutes les facettes du pourriel. Qui plus est, les deux organismes d'application concernés, tout comme la GRC et les autorités policières locales, ont des ressources restreintes et des priorités conflictuelles qui limitent leur capacité d'intervention. L'application

est également entravée par la pénurie chronique d'experts nécessaires pour retracer, mener des enquêtes et intenter des poursuites contre les polluposteurs. Enfin, dans bien des cas, les pouvoirs d'application actuels n'ont pas encore été utilisés, et les mesures législatives qui permettraient d'attaquer certaines facettes du pourriel ont une application trop incertaine ou sont simplement inexistantes.

Le Groupe de travail croit fermement qu'il faut renforcer le processus d'application. Pour ce faire, il faut tout d'abord s'engager politiquement à freiner le pourriel et les activités semblables, non seulement en répondant aux plaintes, mais en menant des enquêtes proactives et en intentant des poursuites contre les polluposteurs. L'augmentation des ressources financières et techniques est essentielle, mais le soutien accordé aux organismes d'application devrait également prendre la forme de mécanismes plus efficaces pour la collecte, la coordination et le traitement des renseignements sur le pourriel, notamment ceux qui sont fournis par les gens qui déposent des plaintes. Le chapitre 7 du présent rapport aborde ces mécanismes. Enfin et surtout, il importe de combler les lacunes du régime juridique et réglementaire qui s'applique au pourriel et aux autres menaces pour Internet, tels les logiciels espions.

Recherche juridique

Pour établir le contexte de ses délibérations, le Groupe de travail a entrepris une analyse des lois anti-pourriel des autres pays, particulièrement des États-Unis, du Royaume-Uni et de l'Australie. L'analyse avait pour but de comparer la situation actuelle du Canada à celle de ces compétences. L'encadré 2 intitulé « Lois internationales anti-pourriel » énonce le titre des lois en vigueur dans quelques pays clés.

Encadré 2 — Lois internationales anti-pourriel

États-Unis — *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CAN-SPAM Act of 2003)

Australie — *Spam Act* 2003

Royaume-Uni — *Privacy and Electronic Communications Regulations* 2003

France — *Loi pour la confiance dans l'économie numérique* 2004

Union européenne — *Directive* 2003/58/CE

En outre, le Groupe de travail a commandé une étude du droit privé d'action contre le pourriel au Canada, qui abordera notamment le cadre législatif existant, les principaux éléments constitutifs d'un tel droit et l'opinion des entreprises canadiennes sur l'importance de ce dernier.

Identification des lacunes législatives

Après avoir examiné les lois et les mécanismes d'application, l'expérience des pays ayant déjà adopté des lois générales anti-pourriel, l'issue des poursuites de ses membres et les leçons retenues, le Groupe de travail a conclu qu'il y avait des lacunes évidentes dans les lois et les mécanismes d'application canadiens.

En effet, bien qu'elles soient applicables à certaines facettes du pollupostage, les dispositions des trois lois pertinentes ne peuvent être utilisées avec suffisamment de certitude pour contrer efficacement les méthodes et les moyens des polluposteurs, les intrusions plus agressives et envahissantes, ni les nouvelles menaces à la sécurité du réseau Internet. Pour leur part, les pouvoirs d'application des organismes sont limités par la portée et les objectifs des lois qui les régissent, et, selon leur libellé actuel, ces lois excluent un grand nombre d'activités de pollupostage et d'activités connexes.

On a cerné une autre lacune sur le plan de la dissuasion. Au regard des lois applicables, on s'est posé la question suivante : « Les sanctions sont-elles suffisamment sévères pour décourager le pollupostage? ». Le Groupe de travail a déterminé que, bien que les mécanismes actuels soient adéquats dans le cas des sociétés légitimes qui se sont adonnées au pollupostage par erreur, il n'est pas évident qu'ils dissuaderaient les véritables contrevenants. En outre, même lorsque des sanctions significatives sont prévues, par exemple dans le *Code criminel*, l'aspect pratique de leur application aux poursuites fondées sur des infractions liées au pourriel est limité.

Un cadre pour les lois anti-pourriel et leur mise en application

Après avoir systématiquement évalué l'utilité des lois et des mesures d'application actuelles à la lumière des menaces posées par le pourriel et les activités connexes, le Groupe de travail a conclu ce qui suit :

- Bien que les lois actuelles traitent de facettes précises du pourriel, elles ne permettent pas, individuellement ou ensemble, d'atteindre l'objectif global, à savoir décourager les polluposteurs au Canada.
- Une loi autonome, neutre quant aux techniques visées et traitant clairement du pourriel, des infractions liées au pourriel et des nouvelles menaces (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) s'impose. Des modifications aux lois actuelles pourraient également s'avérer nécessaires.

Nature des infractions, recours et sanctions

- Le défaut de se conformer à des procédures d'inclusion pour l'envoi de messages électroniques non sollicités devrait constituer une infraction au titre d'une loi anti-pourriel autonome, neutre quant aux techniques visées.
- L'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, l'objectif ou le contenu d'un courriel devrait constituer une infraction et ce, que le but soit de tromper les destinataires ou de contourner les filtres techniques.
- La construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées) devrait constituer une infraction.
- La collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes, devraient constituer une infraction.
- Les attaques de dictionnaire devraient constituer une infraction.
- Les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions susmentionnées.
- Un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile.
- Les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient être tenues également responsables du pourriel. La responsabilité devrait aussi incomber aux tiers qui bénéficient du pourriel.

Administration et application de la loi

- L'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public et l'octroi d'un soutien aux organismes d'application de la loi.
- L'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.
- On devrait augmenter les ressources et l'aide destinées aux organismes responsables de l'application des dispositions anti-pourriel nouvelles et actuelles.
- Étant donné que le pourriel est un problème sans frontière, on devrait prévoir des dispositions favorisant l'application des lois et la tenue d'enquêtes à l'échelle internationale. Toutes les dispositions actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre de démarches anti-pourriel homogènes.

Mesures réglementaires

Bien que les discussions du Groupe de travail aient porté principalement sur l'interdiction du pourriel et des activités connexes, les participants à la Table ronde des intervenants de décembre 2004 et les membres du Groupe de travail ont discuté du bien-fondé de mesures réglementaires plus vastes. Certains favorisaient une démarche coréglementaire fondée sur le modèle australien qui énoncerait les responsabilités des FSI dans des secteurs tels que la protection des réseaux contre le pourriel. D'autres préféraient la pratique canadienne axée sur la coopération volontaire et la pression uniformisante du secteur industriel, mentionnant qu'elle serait une méthode de lutte anti-pourriel plus rapide et efficace que la démarche coréglementaire. Le sujet a été longuement débattu, mais on a convenu à l'unanimité que le gouvernement ne devrait pas dicter de solutions techniques précises et que les règles fondamentales législatives (y compris celles qui sont décrites précédemment) devraient être plus neutres quant aux techniques utilisées et visées.

Le secteur industriel s'efforce déjà de régler le problème du pourriel, mais l'expérience du Groupe de travail démontre que le dialogue gouvernement-secteur industriel peut contribuer à mobiliser les énergies du secteur privé. Par conséquent, le Groupe de travail accorde énormément d'importance à la poursuite du dialogue entre le gouvernement et le secteur industriel dans ce domaine. Il croit également que les questions plus vastes concernant la réglementation d'Internet doivent être étudiées dans le cadre de l'examen de la politique des télécommunications annoncé par le gouvernement du Canada dans le budget fédéral de 2005.

Recommandations

Après avoir analysé la situation canadienne et l'expérience des autres pays, le Groupe de travail a conclu que le Canada ne pourrait pas combattre efficacement le pourriel au pays à moins d'intégrer à sa démarche anti-pourriel multiple, un ensemble de lois plus précises, exhaustives et appliquées de façon active, qui protègent les internautes et favorisent la croissance du cybercommerce.

En conséquence, nos recommandations sont les suivantes :

Recommandation 2 :

Le gouvernement fédéral devrait adopter un ensemble de règlements judiciaires précis, visant à interdire le pourriel et les nouvelles menaces à la sécurité du réseau Internet (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) et, pour ce faire, adopter une nouvelle loi et modifier les lois actuelles au besoin.

Recommandation 3 :

À cette fin, les activités et pratiques de multipostage abusif suivantes devraient constituer des infractions au titre d'une loi anti-pourriel spécifique (ces dispositions peuvent également être énoncées, en totalité ou en partie, dans les lois actuelles) :

- **le défaut de se conformer à des procédures d'inclusion pour l'envoi de courriels non sollicités;**
- **l'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, le but ou le contenu d'un courriel, que l'objectif soit de tromper le destinataire ou de contourner les filtres techniques;**
- **la construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées);**

- **la collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes;**
- **les attaques de dictionnaire.**

Recommandation 4 :

Les sanctions et recours suivants devraient s'appliquer à ces nouvelles infractions :

- **les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions énumérées à la recommandation 3;**
- **un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile;**
- **les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient être tenues également responsables du pourriel. La responsabilité devrait également incomber aux tiers qui bénéficient du pourriel.**

Recommandation 5 :

En ce qui concerne l'application et l'administration de la nouvelle loi :

- **l'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public et l'octroi d'un soutien aux organismes d'application;**
- **l'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.**

Recommandation 6 :

Le gouvernement fédéral devrait accorder la priorité à l'application des mesures anti-pourriel en renforçant le soutien et les ressources destinés aux organismes responsables de l'application des lois anti-pourriel nouvelles et actuelles.

Recommandation 7 :

Le gouvernement fédéral, de concert avec les provinces et les territoires, devrait conclure et mettre en œuvre des accords de coopération en matière d'application des lois avec d'autres pays. Toutes les dispositions législatives actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre d'enquêtes coopératives et de mesures de mise en application homogènes, à l'échelle internationale.

3 GÉRER LES RÉSEAUX POUR CONTRER LE POURRIEL

LE DÉFI

Toute mesure visant à protéger la sécurité des communications Internet de menaces comme les pourriels, les virus et les logiciels espions doit s'appuyer sur autre chose que des démarches gouvernementales. De plus en plus d'intervenants reconnaissent que les FSI et les autres exploitants de réseaux (par exemple les grandes entreprises, les universités et les ministères gouvernementaux) peuvent adopter plusieurs mesures pour rétablir la confiance à l'égard des communications Internet.

Certaines de ces mesures portent sur la mise au point et l'application de la technologie, d'autres sur la mise en œuvre de pratiques exemplaires et de Politiques d'utilisation acceptable interdisant le pourriel au sein du secteur industriel. Elles sont fondées sur un objectif commun : veiller à ce que le courriel reste un outil valable pour les communications d'affaires et personnelles légitimes.

De par sa conception et son architecture, Internet est un « réseau de réseaux » ouvert qui permet la libre circulation de l'information. L'élaboration et la mise en œuvre de nouvelles normes techniques pour améliorer la sécurité et éliminer les abus se poursuivront pendant de nombreuses années.

Certaines pratiques connues de gestion des réseaux peuvent cependant favoriser le pourriel et d'autres formes d'abus du réseau. Par exemple, en laissant les serveurs ouverts pour relayer ou envoyer des messages, on permet que des systèmes informatiques soient la proie de ceux qui les transforment en serveurs mandataires pour le pollupostage. Plusieurs organismes ont entrepris d'avertir les entreprises et les gestionnaires de réseaux de l'importance d'assurer la sécurité des systèmes et des réseaux, mais l'adoption des pratiques proposées reste inégale.

Bien que le problème du pourriel, à l'instar d'Internet, soit un phénomène mondial, des démarches en matière de gestion des réseaux adoptées au Canada peuvent contribuer à le résoudre. Les propriétaires et les gestionnaires de réseaux doivent envisager et adopter des pratiques de gestion qui mettront un frein au pourriel et aux menaces connexes.

Les intervenants du secteur industriel canadien peuvent se mettre d'accord sur des pratiques de base d'exploitation des réseaux qui mettront un frein au pourriel et faire preuve de leadership en exigeant l'adoption de ces pratiques par les installations et réseaux établis au Canada.

Activités du Groupe de travail

La création du Groupe de travail sur le pourriel représente le tout premier effort de collaboration entre un vaste éventail d'organisations, y compris la plupart des plus grands et plus petits FSI à large bande et par réseau commuté, d'autres exploitants de réseaux, les grandes entreprises qui utilisent Internet, les concepteurs de logiciels, les groupes de lutte contre le pourriel et le gouvernement. L'accord des intervenants, en matière de collaboration à l'élaboration et à la mise en œuvre de solutions au problème du pourriel à l'échelle de tout le secteur industriel, représente un énorme accomplissement. Cependant, ce n'est que le début d'un engagement à long terme à l'égard de l'adoption des mesures nécessaires pour mettre fin au pourriel.

Encadré 3 — Pratiques exemplaires recommandées pour les FSI et autres exploitants de réseaux

- Tous les registraires et hôtes canadiens de noms de domaine devraient publier des renseignements sur Sender Policy Framework (SPF) dans les fichiers de leur zone respective de serveur de nom de domaine le plus tôt possible.
- Les FSI et autres exploitants de réseaux devraient limiter, par défaut, l'utilisation du port 25 par les utilisateurs finaux. Au besoin, la capacité d'envoyer ou de recevoir du courriel au moyen du port 25 devrait être limitée aux ordinateurs hôtes du réseau du fournisseur. L'utilisation du port 25 par les utilisateurs finaux devrait être permise au besoin ou être conforme à l'entente entre le fournisseur et l'utilisateur final et aux modalités de service.
- Les FSI et autres exploitants de réseaux devraient bloquer les pièces jointes aux courriels dont les extensions sont connues pour transporter des virus ou filtrer les pièces jointes en fonction des propriétés du contenu.
- Les FSI et autres exploitants de réseaux devraient surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence.
- Les FSI et autres exploitants de réseaux devraient établir et maintenir de façon continue des processus efficaces et rapides pour la gestion et l'élimination des éléments de réseau infectés constituant une source de pourriel.
- Les FSI et autres exploitants de réseaux devraient établir des processus interentreprises pertinents afin de réagir aux rapports d'incidents des autres exploitants de réseaux.
- Les FSI et autres exploitants de réseaux ainsi que les fournisseurs de service de courrier électronique devraient communiquer leurs politiques et procédures en matière de sécurité à leurs abonnés.
- Les FSI et autres exploitants de réseaux devraient adopter la validation du courriel sur tous leurs serveurs Simple Mail Transfer Protocol (SMTP) (c'est-à-dire entrée, sortie, relais).
- Les avis de non-remise (NDN) ne devraient être envoyés que dans les cas de courriels légitimes.
- Les FSI et autres exploitants de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers de systèmes de noms de domaine (DNS) et les fichiers d'enregistrement d'adresse IP applicables (WHOIS/SWIP/RWHOIS) soient maintenus à jour à l'aide de renseignements corrects, complets et courants. Ces renseignements devraient comprendre les points de contact responsables de résoudre les questions d'abus et inclure, sans toutefois s'y limiter, les adresses postales, les numéros de téléphone et les adresses de courriel.
- Les FSI et autres exploitants de réseaux devraient veiller à ce que leurs adresses routables publiques et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP. Tous les exploitants de réseau local d'entreprise (RLE) devraient se conformer au document Request for Comments (RFC) 1918 — « Address Allocation for Private Internets ». Les RLE, plus particulièrement, ne devraient pas utiliser l'espace IP enregistré globalement à quelqu'un d'autre ou l'espace IP non enregistré à quelqu'un, à titre d'espace IP privé.
- Les FSI et autres exploitants de réseaux devraient interdire l'envoi de courriels renfermant des en-têtes frauduleux ou contrefaits. L'en-tête de message devrait être exact et conforme aux documents RFC pertinents, notamment le RFC 822 et le RFC 2822, et les domaines de référence et les adresses IP devraient comporter des données d'enregistrement exactes et à jour.

Pratiques exemplaires recommandées pour les fournisseurs de service Internet et autres exploitants de réseaux

Le Groupe de travail a élaboré une série de pratiques exemplaires techniques recommandées pour aider à réduire le pourriel au Canada. L'encadré 3 ci-dessus présente les points saillants de ce document. L'adoption de ces pratiques servira en même temps à s'attaquer aux problèmes de sécurité associés au pourriel, puisque celui-ci est souvent le véhicule d'activités plus nuisibles. Les pratiques représentent une continuation des efforts et des progrès accomplis dans ce secteur depuis quelque temps au Canada et à l'échelle internationale. Le Groupe de travail a cependant amplifié ces travaux en établissant le premier consensus vraiment national sur des mesures techniques recommandées pour combattre le pourriel. Ces pratiques exemplaires dotent le Canada d'un modèle qu'il pourra partager à l'échelle internationale dans la lutte mondiale contre le pourriel. Il faudra, toutefois, actualiser continuellement ces pratiques afin qu'elles reflètent l'évolution constante des tendances et des techniques relatives au pourriel.

Le texte complet des pratiques exemplaires recommandées par le Groupe de travail se trouve à l'appendice B.

Mesurer la mise en œuvre et les répercussions

Un grand nombre de FSI canadiens, y compris plusieurs joueurs importants et autres exploitants de réseaux, ont commencé à mettre en œuvre la totalité ou une partie des pratiques techniques recommandées, notamment le blocage du port 25 et la mise à niveau de leurs techniques de filtrage.

- Tous les registraires et hôtes canadiens de noms de domaine devraient publier des renseignements sur Sender Policy Framework (SPF) dans les fichiers de leur zone respective de serveur de nom de domaine le plus tôt possible.
- Les FSI et autres exploitants de réseaux devraient limiter, par défaut, l'utilisation du port 25 par les utilisateurs finaux. Au besoin, la capacité d'envoyer ou de recevoir du courriel au moyen du port 25 devrait être limitée aux ordinateurs hôtes du réseau du fournisseur. L'utilisation du port 25 par les utilisateurs finaux devrait être permise au besoin ou être conforme à l'entente entre le fournisseur et l'utilisateur final et aux modalités de service.
- Les FSI et autres exploitants de réseaux devraient bloquer les pièces jointes aux courriels dont les extensions sont connues pour transporter des virus ou filtrer les pièces jointes en fonction des propriétés du contenu.
- Les FSI et autres exploitants de réseaux devraient surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence.
- Les FSI et autres exploitants de réseaux devraient établir et maintenir de façon continue des processus efficaces et rapides pour la gestion et l'élimination des éléments de réseau infectés constituant une source de pourriel.
- Les FSI et autres exploitants de réseaux devraient établir des processus interentreprises pertinents afin de réagir aux rapports d'incidents des autres exploitants de réseaux.
- Les FSI et autres exploitants de réseaux ainsi que les fournisseurs de service de courrier électronique devraient communiquer leurs politiques et procédures en matière de sécurité à leurs abonnés.
- Les FSI et autres exploitants de réseaux devraient adopter la validation du courriel sur tous leurs serveurs Simple Mail Transfer Protocol (SMTP) (c'est-à-dire entrée, sortie, relais).
- Les avis de non-remise (NDN) ne devraient être envoyés que dans les cas de courriels légitimes.
- Les FSI et autres exploitants de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers de systèmes de noms de domaine (DNS) et les fichiers d'enregistrement d'adresse IP applicables (WHOIS/SWIP/RWHOIS) soient maintenus à jour à l'aide de renseignements corrects, complets et courants. Ces renseignements devraient comprendre les points de contact responsables de résoudre les questions d'abus et inclure, sans toutefois s'y limiter, les adresses postales, les numéros de téléphone et les adresses de courriel.
- Les FSI et autres exploitants de réseaux devraient veiller à ce que leurs adresses routables publiques et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP. Tous les exploitants de réseau local d'entreprise (RLE) devraient se conformer au document Request for Comments (RFC) 1918 — « Address Allocation for Private Internets ». Les RLE, plus particulièrement, ne devraient pas utiliser l'espace IP enregistré globalement à quelqu'un d'autre ou l'espace IP non enregistré à quelqu'un, à titre d'espace IP privé.
- Les FSI et autres exploitants de réseaux devraient interdire l'envoi de courriels renfermant des en-têtes frauduleux ou contrefaits. L'en-tête de message devrait être exact et conforme aux documents RFC pertinents, notamment le RFC 822 et le RFC 2822, et les domaines de référence et les adresses IP devraient comporter des données d'enregistrement exactes et à jour.

Le Groupe de travail a élaboré une série de pratiques exemplaires techniques recommandées pour aider à réduire le pourriel au Canada. L'encadré 3 ci-dessus présente les points saillants de ce document. L'adoption de ces pratiques servira en même temps à s'attaquer aux problèmes de sécurité associés au pourriel, puisque celui-ci est souvent le véhicule d'activités plus nuisibles. Les pratiques représentent une continuation des efforts et des progrès accomplis dans ce secteur depuis quelque temps au Canada et à l'échelle internationale. Le Groupe de travail a cependant amplifié ces travaux en établissant le premier consensus vraiment national sur des mesures techniques recommandées pour combattre le pourriel. Ces pratiques exemplaires dotent le Canada d'un modèle qu'il pourra partager à l'échelle internationale dans la lutte mondiale contre le pourriel. Il faudra, toutefois, actualiser continuellement ces pratiques afin qu'elles reflètent l'évolution constante des tendances et des techniques relatives au pourriel.

Le texte complet des pratiques exemplaires recommandées par le Groupe de travail se trouve à l'appendice B.

Un grand nombre de FSI canadiens, y compris plusieurs joueurs importants et autres exploitants de réseaux, ont commencé à mettre en œuvre la totalité ou une partie des pratiques techniques recommandées, notamment le blocage du port 25 et la mise à niveau de leurs techniques de filtrage.

L'expérience des autres pays a démontré que les FSI, particulièrement les leaders du marché, peuvent favoriser l'adoption de pratiques exemplaires techniques et commerciales anti-pourriel au sein du secteur industriel. En fait, certains FSI canadiens ont déjà mis en œuvre les pratiques exemplaires recommandées, et leur esprit d'initiative a encouragé d'autres FSI à faire de même.

Tout cela semble prometteur, mais il faudra surveiller systématiquement la mise en œuvre des pratiques exemplaires recommandées, afin d'en évaluer les répercussions et de repérer les nouveaux problèmes qui pourraient exiger des amendements ou des ajouts aux dispositions des pratiques exemplaires. À défaut de cela, le secteur industriel, les décideurs gouvernementaux et les autres intervenants auront de la difficulté à déterminer le niveau d'adoption des pratiques recommandées ou à évaluer leur contribution à la lutte anti-pourriel.

Le secteur industriel ayant fait valoir qu'il peut s'autoréglementer, le Groupe de travail encourage les principaux FSI et exploitants de réseaux à continuer à faire preuve de leadership par la mise en œuvre des pratiques exemplaires recommandées et à encourager les autres à suivre leur exemple.

Le Groupe de travail invite également les principaux joueurs et les associations concernées du secteur industriel à s'associer à l'organisme de coordination décrit au chapitre 7, pour élaborer un système efficace de mesure et de rapport public des répercussions des pratiques exemplaires recommandées.

Base de données canadienne sur les pourriels (« congélateur à pourriels »)

Le Groupe de travail a examiné la possibilité d'établir, dans le cadre d'un partenariat des secteurs public et privé, une base de données canadienne sur les pourriels ou « congélateur à pourriels », dont la conception serait semblable à la base de données « réfrigérateur à pourriels » que maintient et gère la Federal Trade Commission (FTC) des États-Unis.

La base de données canadienne servirait d'archivage des copies de pourriels arrivés dans les boîtes aux lettres électroniques. Un organisme canadien chargé de coordonner la lutte anti-pourriel inventorierait ces pourriels et les conserverait pour une période de temps donnée.

Ainsi, les organismes d'application de la loi du Canada et, éventuellement, des autres pays, les FSI, les autres exploitants de réseaux et les divers paliers de gouvernement auraient accès à des données à des fins d'analyse statistique et de collecte de preuves pour l'application des lois anti-pourriel.

Pourriel acheminé sur les appareils sans fil

Contrairement à Internet qui a été conçu comme un réseau ouvert et public, les technologies mobiles ont été originellement déployées sur des réseaux privés et fermés.

Cependant, vu la convergence des technologies et l'interaction accrue entre Internet et les technologies mobiles, certains problèmes qui, à l'origine, affectaient uniquement Internet, commencent à toucher les réseaux mobiles. Ces problèmes sont associés à la récupération du courriel (y compris du pourriel) au moyen d'appareils mobiles. Ils découlent également de la réception de nouvelles formes de pourriel émanant des réseaux sans fil et transmis par messagerie texte, messagerie multimédia et messagerie instantanée aux combinés sans fil. Applications réussies de la technologie mobile, ces services de messagerie ouvrent la voie à des services innovateurs, mais fournissent de nouvelles possibilités aux polluposteurs.

Le pourriel dit « mobile » ou « sans fil » peut poser des problèmes plus graves que le pourriel envoyé aux ordinateurs de bureau car il suit le client, et ce dernier paie parfois des frais pour chaque message reçu. Très gênant pour les abonnés des services mobiles, le pourriel sans fil pourrait devenir beaucoup plus dérangeant que le pourriel envoyé à un ordinateur personnel.

Le Groupe de travail a consulté le secteur des communications sans fil canadien pour discuter du problème et envisager des mesures aptes à empêcher le pourriel de devenir un problème majeur pour les réseaux sans fil. Lors de ces entretiens, il a appris que les exploitants des réseaux sans fil considèrent le pourriel émanant des réseaux sans fil comme une menace grave. Pour protéger ses clients, le secteur des communications sans fil est d'ailleurs en train de mettre en place des mesures techniques et il envisage également des recours juridiques et réglementaires qui pourraient contribuer à prévenir le pourriel mobile.

Le Groupe de travail et les représentants du secteur des communications sans fil ont convenu que toute mesure anti-pourriel adoptée par le gouvernement fédéral et autres parties concernées, suite aux travaux et aux recommandations du Groupe de travail, devrait être neutre quant aux techniques utilisées et visées, et s'appliquer au secteur des communications sans fil au moyen de mécanismes appropriés.

Partage des renseignements techniques entre les fournisseurs de services Internet et les autres exploitants de réseaux

Le secteur industriel a accompli beaucoup de travail pour endiguer le pourriel et ses efforts ont mené à des améliorations notoires, mais il reste encore beaucoup à faire sur le plan de la collaboration.

Un meilleur partage des renseignements entre les FSI et les autres exploitants de réseaux représente un facteur clé de succès. La lutte anti-pourriel repose sur une démarche concertée à l'égard des problèmes, axée notamment sur une communication rapide et efficace des questions et problèmes d'intérêt commun et sur l'établissement de procédures intersociétés appropriées pour répondre aux rapports d'incidents.

Recommandations

Les FSI et autres exploitants de réseaux sont aux premières lignes de la lutte anti-pourriel. Point de contact entre les expéditeurs et les destinataires du pourriel, ils sont dans une position unique pour combattre le pourriel.

En conséquence, nos recommandations sont les suivantes :

Recommandation 8 :

Les FSI et autres exploitants de réseaux devraient mettent en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel.

Recommandation 9 :

Les FSI et autres exploitants de réseaux, en coopération avec l'organisme de coordination établi par le ministre de l'Industrie (mentionné à la recommandation 5), devraient mesurer de façon continue l'ampleur du problème du pourriel au Canada et évaluer les répercussions des pratiques recommandées. Ils devraient continuer à cerner les questions qui pourraient mériter davantage d'examen et mener à la formulation de recommandations additionnelles.

Recommandation 10 :

Afin de faciliter de façon continue la surveillance des tendances du pourriel et l'élaboration de mesures et de techniques anti-pourriel, le gouvernement devrait jouer un rôle de leadership en créant une base de données canadienne sur les pourriels (« congélateur à pourriels »).

Recommandation 11 :

Les FSI et autres exploitants de réseaux devraient adopter et appliquer des Politiques d'utilisation acceptable interdisant clairement le pollupostage sur leurs réseaux.

4 RÉTABLIR LA CONFIANCE À L'ÉGARD DU COURRIEL

LE DÉFI

Avant la mise sur pied du Groupe de travail sur le pourriel, la majorité des initiatives canadiennes visant à endiguer le volume croissant de courriels commerciaux non sollicités associaient des technologies de filtrage et le recours aux « listes noires » de serveurs et de domaines identifiés comme étant des sources de pourriel. Cependant, à mesure que ces services de contrôle du pourriel se perfectionnent, les polluposteurs se montrent eux-mêmes très ingénieux lorsqu'il s'agit de trouver de nouvelles façons de contourner les obstacles qu'on leur crée.

Les diverses technologies de filtrage et outils de blocage utilisés par les FSI et autres exploitants de réseaux, de même que les batailles cycliques entre polluposteurs et services de filtrage de pourriel, ont eu des effets non désirés. Les courriels commerciaux légitimes, comme les courriels non commerciaux et les courriels personnels légitimes, sont souvent interceptés par les filtres, parfois à l'insu de l'expéditeur ou du destinataire. Ces pratiques et techniques de filtrage, bien que mises en œuvre dans un but fort louable, ont donc contribué indirectement à miner la confiance du consommateur à l'égard de la fiabilité du courriel.

Pour cette raison, certains organismes commerciaux envisagent maintenant de se tourner vers des réseaux fermés, ce qui minerait l'utilisation efficace d'Internet comme plate-forme pour le commerce. On peut comprendre les motifs pour lesquels ils envisagent cette solution, mais l'abandon du réseau public Internet en faveur de réseaux privés pour les activités commerciales pourrait avoir des effets indésirables.

Des choix moins radicaux que le réseau fermé commencent à s'offrir sous la forme de techniques favorisant la circulation des courriels commerciaux légitimes plutôt que le filtrage des communications non désirées. Bien que l'utilisation de ces techniques puisse entraîner des frais pour les expéditeurs de courriels commerciaux et les propriétaires et gestionnaires de réseaux Internet, ces coûts seraient plus que contrebalancés par les avantages suivants :

- pour les expéditeurs de courriels commerciaux, une livraison améliorée;
- pour les fournisseurs de services, une réduction des frais de gestion du service de courriel et des préférences des clients;
- pour les utilisateurs du courriel, des outils de gestion du courriel plus efficaces.

La certification est une des techniques envisagées pour améliorer la livraison. L'obligation pour l'expéditeur de divulguer sa véritable identité et la nature de sa communication constituerait une exigence minimale pour l'établissement d'un régime de certification du courriel. Un tel régime devrait aussi prévoir un solide moyen de mesurer l'efficacité de la méthode ainsi que des sanctions appropriées s'appliquant aux détenteurs de certificats qui enfreignent les règles.

Outre la certification, on dispose maintenant de techniques qui facilitent la circulation du courriel légitime en authentifiant les sites d'envoi et de réception. Cependant, ces techniques ne protègent pas nécessairement les destinataires des courriels faux, trompeurs et frauduleux provenant de sites authentiques.

À l'instar des autres éléments de la boîte à outils anti-pourriel, les techniques établies, telles que les listes noires et le filtrage, et les nouvelles techniques, notamment la certification et l'authentification, ne permettront pas de régler tous les problèmes de livraison du jour au lendemain. Mais, outre ces solutions techniques, les expéditeurs de courriels commerciaux peuvent adopter diverses pratiques commerciales aptes à endiguer le volume de pourriel et les menaces pour Internet. Pour le milieu du commerce par courriel, le défi consiste à cerner et à mettre en œuvre une combinaison gagnante de pratiques commerciales appropriées et de solutions techniques efficaces.

Activités du Groupe de travail

Le groupe de travail a d'abord réuni un groupe d'intervenants qui n'avaient jamais travaillé ensemble par le passé, pour discuter des questions que pose le pourriel aux expéditeurs de courriels légitimes et trouver des façons d'améliorer la livraison du courriel commercial légitime.

Outre les mesures décrites dans la section précédente, diverses mesures techniques et commerciales peuvent être adoptées pour lutter contre le pourriel et améliorer la livraison du courriel légitime. Par conséquent, le Groupe de travail a décidé de consacrer une partie importante de ses travaux à l'élaboration de pratiques exemplaires pour les expéditeurs de courriels, notamment l'identification des mesures opérationnelles et techniques à prendre pour améliorer la livraison de leurs messages.

Ayant conclu que l'Internet Engineering Task Force et ses groupes de travail coordonnaient efficacement l'élaboration de techniques d'authentification, le Groupe de travail a décidé d'axer ses efforts sur les mesures techniques concernant l'exploration des techniques de certification du courriel ainsi que sur la sensibilisation à l'apport éventuel de ces techniques à la livraison du courriel et d'encourager également un débat entre les segments du secteur industriel.

Pratiques exemplaires recommandées pour le marketing par courriel

Les pratiques exemplaires recommandées pour les expéditeurs de courriels commerciaux formulées par le Groupe de travail reflètent les dispositions d'un cadre législatif et d'un code d'autoréglementation déjà en vigueur au Canada.

- La LPRPDE, entrée en vigueur au Canada en janvier 2004, énonce les obligations des personnes qui recueillent, emmagasinent et utilisent les adresses de courriels considérées comme des renseignements personnels.
- L'Association canadienne du marketing possède un code de déontologie obligatoire depuis plusieurs années. Les organismes qui effectuent des sondages en ligne, c'est-à-dire les membres du Conseil canadien de la recherche par sondage, élaborent actuellement un code de pratique uniforme.

S'inspirant de ces documents et des codes de pratiques élaborés par d'autres compétences (par l'Anti-Spam Technical Alliance des États-Unis par exemple), le Groupe de travail a rédigé un ensemble de pratiques exemplaires visant à encourager les expéditeurs de courriels commerciaux canadiens à adopter des techniques de marketing et autres pratiques commerciales qui ne font pas appel au pourriel et à leur faire comprendre que le pourriel n'a aucunement sa place dans le commerce électronique au Canada.

Le texte complet des pratiques exemplaires figure à l'appendice C. Les points saillants sont présentés à l'encadré 4.

Livraison des courriels commerciaux

Malgré une abondance de preuves, il y a un manque de statistiques sur l'ampleur du problème de livraison, c'est-à-dire le volume de courriels commerciaux légitimes interceptés par les programmes et les services de filtrage – un processus qui génère ce que l'on appelle des « résultats faux positifs » (c'est-à-dire des messages interceptés qui ne sont pas du pourriel). Une étude menée récemment par le cabinet Return Path a révélé qu'en 2004, 22 p. 100 des courriels commerciaux dont la livraison était autorisée, n'avaient pas atteint les destinataires prévus.

- Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.
- Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.
- Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.
- Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.
- Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'usager ou d'autres techniques de surveillance des sites Web.
- Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.
- Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.
- Lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu.
- Tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.
- Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.
- Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :
  - ils ont obtenu leur consentement;
  - ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou la prestation de services associés à cet achat);
  - les destinataires savent pourquoi ils reçoivent des courriels;
  - il y a un moyen facile de refuser de recevoir davantage de courriels.

Les résultats faux positifs posent un problème, d'une part aux entreprises en entravant l'efficacité du courriel comme outil de marketing, et d'autre part aux utilisateurs finaux qui comptent de plus en plus sur la livraison des courriels à destination et en provenance de sources professionnelles (par exemple, collègues de travail), commerciales (par exemple, suite au marketing et à des achats en ligne qu'ils ont effectués) ou personnelles (par exemple, correspondance privée).

Les entreprises de marketing et autres ont de plus en plus recours à des entreprises imparties spécialisées dans la livraison de leur courriel pour améliorer le rendement de leur investissement ou à l'embauche de personnel à temps plein pour traiter de ces questions.

Les FSI devraient envisager de publier des politiques et des procédures claires à l'égard du courriel d'arrivée, et de fournir des points de contact pour améliorer la livraison du courriel légitime.

Plusieurs des grands sites de réception, notamment AOL®, MSN® Hotmail et Yahoo!®, ont publié des politiques et procédures décrivant les exigences applicables aux expéditeurs de courriels légitimes souhaitant figurer sur une liste blanche. Le contournement des filtres anti-pourriel, grâce à ce statut, varie d'un site à l'autre.

Plusieurs techniques sont actuellement utilisées pour lutter contre le pourriel, mais certaines d'entre elles ne peuvent pas toujours distinguer le courriel légitime du pourriel. Par exemple, certains filtres anti-pourriel interceptent les envois en vrac de courriels légitimes simplement parce qu'ils ressemblent au pourriel. D'autres analysent le contenu des messages à l'aide de mots clés utilisés dans le courriel légitime et le pourriel pour déterminer s'ils doivent ou non être filtrés. Pour compliquer les choses davantage, il arrive que les polluposteurs déguisent leurs messages en courriels légitimes et utilisent d'autres techniques pour déjouer les filtres.

Tel que mentionné dans la section de ce chapitre intitulée « Le défi », la certification du courriel pourrait éventuellement permettre aux filtres anti-pourriel d'autoriser la livraison du courriel légitime aux destinataires prévus. Elle pourrait également servir à distinguer le courriel légitime du courriel hameçon.

Encadré 4 — Pratiques exemplaires recommandées pour le marketing par courriel

- Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.
- Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.
- Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.
- Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.
- Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'usager ou d'autres techniques de surveillance des sites Web.
- Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.
- Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.
- Lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu.
- Tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.
- Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.
- Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :
  - ils ont obtenu leur consentement;
  - ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou la prestation de services associés à cet achat);
  - les destinataires savent pourquoi ils reçoivent des courriels;
  - il y a un moyen facile de refuser de recevoir davantage de courriels.

Les résultats faux positifs posent un problème, d'une part aux entreprises en entravant l'efficacité du courriel comme outil de marketing, et d'autre part aux utilisateurs finaux qui comptent de plus en plus sur la livraison des courriels à destination et en provenance de sources professionnelles (par exemple, collègues de travail), commerciales (par exemple, suite au marketing et à des achats en ligne qu'ils ont effectués) ou personnelles (par exemple, correspondance privée).

Les entreprises de marketing et autres ont de plus en plus recours à des entreprises imparties spécialisées dans la livraison de leur courriel pour améliorer le rendement de leur investissement ou à l'embauche de personnel à temps plein pour traiter de ces questions.

Les FSI devraient envisager de publier des politiques et des procédures claires à l'égard du courriel d'arrivée, et de fournir des points de contact pour améliorer la livraison du courriel légitime.

Plusieurs des grands sites de réception, notamment AOL®, MSN® Hotmail et Yahoo!®, ont publié des politiques et procédures décrivant les exigences applicables aux expéditeurs de courriels légitimes souhaitant figurer sur une liste blanche. Le contournement des filtres anti-pourriel, grâce à ce statut, varie d'un site à l'autre.

Certification du courriel

Plusieurs techniques sont actuellement utilisées pour lutter contre le pourriel, mais certaines d'entre elles ne peuvent pas toujours distinguer le courriel légitime du pourriel. Par exemple, certains filtres anti-pourriel interceptent les envois en vrac de courriels légitimes simplement parce qu'ils ressemblent au pourriel. D'autres analysent le contenu des messages à l'aide de mots clés utilisés dans le courriel légitime et le pourriel pour déterminer s'ils doivent ou non être filtrés. Pour compliquer les choses davantage, il arrive que les polluposteurs déguisent leurs messages en courriels légitimes et utilisent d'autres techniques pour déjouer les filtres.

Tel que mentionné dans la section de ce chapitre intitulée « Le défi », la certification du courriel pourrait éventuellement permettre aux filtres anti-pourriel d'autoriser la livraison du courriel légitime aux destinataires prévus. Elle pourrait également servir à distinguer le courriel légitime du courriel hameçon.

En collaboration avec le Conseil consultatif canadien sur les normes de technologies de l'information et des télécommunications, le Groupe de travail sur le pourriel a examiné les régimes de certification existant au Canada, leurs principes, leurs modèles fonctionnels et leurs techniques. Un document de référence présentera les résultats de cette analyse et examinera ensuite les possibilités inhérentes à la mise en œuvre d'un régime de certification du courriel au Canada.

Recommandations

Les expéditeurs de courriels commerciaux sont ceux qui ont le plus à perdre et le plus à gagner dans la lutte anti-pourriel. De plus, parmi les divers groupes d'intervenants engagés dans la lutte anti-pourriel, ce sont ces expéditeurs de courriels commerciaux qui auront sans doute le plus de difficultés à s'organiser pour entreprendre des démarches concertées contre les polluposteurs et à participer à la mise en œuvre de l'approche de type « boîte à outils ».

Le groupe des intervenants composés des expéditeurs de courriels commerciaux rassemble des organismes très distincts, notamment :

- les entreprises qui ont recours au courriel de masse non sollicité pour commercialiser leurs produits et services;
- les entreprises de marketing par courriel;
- les concepteurs et gestionnaires de campagnes de marketing;
- les fournisseurs de services de courriel commercial;
- les fournisseurs de listes d'adresses de courriel.

Certaines sociétés qui fournissent ces produits et services sont verticalement intégrées dans divers segments de la chaîne de production du courriel commercial. D'autres sont autonomes et exercent leurs activités sur une base contractuelle.

La plupart des sociétés du groupe des intervenants composés des expéditeurs de courriels commerciaux exercent leurs activités dans le respect des lois et conformément aux pratiques commerciales généralement reconnues. Comme l'ont démontré les causes jugées en vertu de la LPRPDE, ces sociétés s'empressent généralement d'offrir compensation s'il est constaté qu'elles se sont adonnées à des activités ou à des pratiques contraires à ces normes.

Malheureusement, chaque segment de la chaîne de production du courriel compte des polluposteurs, entreprises et particuliers qui enfreignent de façon délibérée les lois interdisant l'envoi de courriels commerciaux non sollicités ou qui se servent du courriel pour s'adonner à des activités destinées à tromper le public, à endommager les ordinateurs et les réseaux, et à s'approprier des renseignements personnels à des fins frauduleuses.

Pour arrêter le pourriel, il faut arrêter les polluposteurs. À défaut d'y arriver, nous risquons que les Canadiens perdent confiance en l'utilité d'Internet pour le marketing et la promotion des produits et services, et comme moyen efficace de communication. Or, une perte générale de confiance à l'égard du courriel, d'une part, entraverait sérieusement l'émergence d'une cyberéconomie au Canada et d'autre part, nuirait aux intérêts des nombreuses entreprises, organismes, institutions et instances gouvernementales associées à la chaîne de production du courriel professionnel.

En conséquence, nos recommandations sont les suivantes :

Recommandation 12 :

Les entreprises de marketing par courriel devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel et, de concert avec l'organisme de coordination mis sur pied par le ministre de l'Industrie, devraient évaluer continuellement l'efficacité de ces pratiques.

Recommandation 13 :

Le secteur industriel canadien, en coordination avec les organismes internationaux d'élaboration de normes, devrait continuer d'étudier diverses méthodes de certification et leurs frais connexes pour déterminer quelle méthode, s'il en est, constituerait le régime de certification le plus approprié au Canada.

Recommandation 14 :

Pour déterminer la portée du problème de non-livraison du courriel légitime au Canada, l'organisme de coordination mis sur pied par le ministre de l'Industrie devrait étudier officiellement cette question de façon permanente, avec l'aide des intervenants appropriés.

5 SENSIBILISATION DU PUBLIC

LE DÉFI

Les législateurs, les organismes d'application de la loi, les FSI et les autres exploitants de réseaux, ainsi que les utilisateurs du courriel commercial peuvent prendre une part très active à la lutte contre le pourriel. Toutefois, on s'entend généralement pour dire que tous les utilisateurs finaux d'Internet, les employés, les étudiants et les consommateurs ont un rôle important à jouer dans la lutte constante contre ce fléau.

Par ailleurs, pour aider les internautes à remplir leur rôle, on doit de toute évidence mieux les renseigner sur les mesures s'offrant à eux afin de limiter le volume de courriels commerciaux indésirables qu'ils reçoivent, se protéger et protéger les autres utilisateurs contre les virus, échapper aux pratiques frauduleuses et empêcher que des pirates ne contrôlent leur ordinateur pour envoyer des pourriels à leur insu.

L'information abonde sur les mesures que peuvent prendre les utilisateurs afin de limiter le volume de pourriels qu'ils reçoivent et échapper aux pratiques trompeuses et frauduleuses ou aux autres pratiques criminelles associées à ces pourriels. Toutefois, il ressort des sondages d'opinion publique que l'on doit redoubler d'efforts pour diffuser ces renseignements, en particulier ceux qui concernent les nouvelles menaces risquant de perturber le fonctionnement des appareils, de léser les consommateurs et de compromettre la sécurité d'Internet.

Les utilisateurs n'ont pas tous reçu ou compris certains messages très simples, comme « n'ouvrez pas les courriels non sollicités », « n'effectuez aucun achat auprès des polluposteurs » et « ne transmettez pas de renseignements personnels si vous ne connaissez pas avec certitude l'identité du destinataire ». Par exemple, selon *The Ipsos Trend Report Canada* de mai-juin 2004 publié par Ipsos-Reid, plus du tiers des Canadiens branchés ouvrent les pourriels qu'ils reçoivent, et la curiosité constitue la principale raison invoquée à cet égard.

Une étude menée récemment par Option consommateurs a par ailleurs indiqué que certains groupes pourraient bénéficier d'une intensification des activités d'éducation et de sensibilisation adaptées à leurs besoins particuliers, entre autres les personnes de moins de 30 ans qui ont déclaré recevoir davantage de pourriels que les autres groupes et les personnes âgées.

Compte tenu qu'un faible taux de participation des consommateurs suffit pour assurer la viabilité commerciale des activités de pollupostage, l'approche de type boîte à outils doit mettre davantage en évidence le lien existant entre le volume de pourriels et le comportement des consommateurs.

En raison du lien direct qui les unit aux internautes, les FSI et les vendeurs légitimes de produits et services sont bien placés afin de mener une campagne d'éducation et de sensibilisation du public en partenariat avec les groupes de défense des consommateurs et les gouvernements. Pour le Groupe de travail sur le pourriel, le défi consistait donc à faciliter l'élaboration d'une campagne de marketing social et de communications s'adressant aux utilisateurs et à la mettre en œuvre en collaboration avec des groupes de défense des consommateurs, des ministères et organismes gouvernementaux et des partenaires internationaux intéressés.

Activités du Groupe de travail

En plus d'examiner la recherche actuelle sur l'opinion des consommateurs concernant les pourriels, le Groupe de travail a analysé les campagnes d'éducation et de sensibilisation en cours au Canada et dans d'autres pays. Plusieurs de ces initiatives ont bénéficié d'une visibilité limitée, mais les principaux messages véhiculés n'étaient pas toujours uniformes. Après l'examen de la recherche et des initiatives, le Groupe de travail a élaboré une stratégie de communications globale afin de définir les objectifs, les publics cibles et les outils nécessaires à une campagne potentielle d'éducation à grande échelle pour renseigner le public sur le pourriel.

Campagne « Arrêtez le pourriel ici / Stop Spam Here »

La première étape de la stratégie fut la mise sur pied d'une campagne bilingue d'éducation des utilisateurs dans Internet. Le succès de cette initiative reposait sur la formulation de messages clés cohérents, présentés de façon uniforme, et sur une vaste diffusion de trois conseils clés, par un large éventail de partenaires, pour aider les utilisateurs à se protéger et à lutter contre le pourriel.

En collaboration avec des spécialistes des communications et du marketing, le Groupe de travail sur le pourriel a conçu une icône que les partenaires pouvaient afficher dans leur site Web et qui renfermait un lien donnant accès aux conseils à l'intention des utilisateurs, affichés à **http://arretezlepourrielici.ca** et **http://stopspamhere.ca**. On trouve dans les deux versions du site Web la marche à suivre afin de participer à la campagne.

Le Groupe de travail a recruté des partenaires gouvernementaux et non gouvernementaux pour afficher l'icône dans leur site Web.

Les organismes des secteurs privé et public et la population en général ont répondu en grand nombre à la campagne « Arrêtez le pourriel ici / Stop Spam Here ». Entre le 25 novembre 2004, date de son entrée en service, et avril 2005, le site a reçu plus de 500 000 visites, et quelque 200 organismes ont participé à la campagne.

Recommandations

La campagne « Arrêtez le pourriel ici / Stop Spam Here » a commencé à éduquer les internautes canadiens sur les moyens qui s'offrent à eux pour réduire le volume de pourriels se retrouvant dans leur boîte de réception et échapper aux pratiques trompeuses, nuisibles, frauduleuses ou autrement illégales associées à certains types de pourriels.

Toutefois, il reste encore beaucoup à faire afin de permettre aux Canadiens de jouer leur rôle dans la lutte contre le pourriel, à commencer par l'amélioration du site Web « Arrêtez le pourriel ici / Stop Spam Here » et la diffusion de l'information qui s'y trouve dans d'autres médias.

Les messages d'ordre général qui s'appliquent à tous les consommateurs, tels que les trois conseils clés présentés ci-dessous, fournissent une base solide pour l'éducation et la sensibilisation du public. Toutefois, d'après le Groupe de travail, il faut aussi mener des campagnes d'éducation et de sensibilisation concordant avec les besoins et les intérêts particuliers de différents groupes de la population canadienne, afin de continuer à progresser.

Arrêtez le pourriel ici : trois conseils clés

1. Protégez votre ordinateur

Le pourriel est une source croissante de virus informatiques. Il est essentiel que vous protégiez votre ordinateur contre les messages transportant des virus. Installez un logiciel anti-virus et anti-pourriel et mettez-le à jour régulièrement. Procurez-vous aussi la protection supplémentaire d'un coupe-feu.

2. Protégez votre adresse de courriel

Réservez une adresse de courriel pour les contacts personnels et professionnels en qui vous avez confiance. Créez une adresse de courriel extensible distincte pour d'autres utilisations en ligne.

3. Protégez-vous

N'essayez rien, n'achetez rien et ne répondez pas aux pourriels. Supprimez-les. C'est une bonne façon de ne pas en recevoir d'autres dans l'avenir.

Le Groupe de travail estime qu'il est primordial de faire participer les petites et moyennes entreprises à la lutte contre le pourriel, car elles seront parmi les plus grands bénéficiaires d'un environnement commercial électronique exempt de pourriels.

C'est pourquoi nous formulons les recommandations suivantes :

Recommandation 15 :

Dans le cadre des efforts continus qu'il déploie pour accroître la sensibilisation et l'éducation des utilisateurs, le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de promouvoir la campagne axée sur les conseils aux utilisateurs « Arrêtez le pourriel ici / Stop Spam Here », en encourageant les responsables d'autres sites Web à placer dans leur site un lien qui y donne accès et en utilisant d'autres méthodes et médias appropriés.

Recommandation 16 :

Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de maintenir et d'enrichir les deux versions du site Web « Arrêtez le pourriel ici / Stop Spam Here ». Le but est d'en faire un mécanisme plus efficace comme outil d'éducation et source de liens utiles donnant accès à d'autres ressources de lutte contre le pourriel, et de veiller à ce que les deux versions demeurent à jour et pertinentes (par exemple, en y affichant de l'information sur les pratiques exemplaires du secteur industriel, la future législation anti-pourriel et les procédures à suivre pour déposer une plainte).

Recommandation 17 :

Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait élaborer des campagnes de sensibilisation et d'éducation efficaces et cohérentes adaptées aux besoins de différents groupes de destinataires cibles en matière de lutte contre le pourriel.

6 RÉSOUDRE UN PROBLÈME MONDIAL

LE DÉFI

Selon les estimations, une faible proportion des pourriels reçus par les Canadiens provient du Canada. Cela s'explique par la nature ouverte d'Internet, qui fait en sorte que les pourriels peuvent être acheminés entre n'importe quels endroits de la planète. Par conséquent, l'harmonisation des politiques anti-pourriel ainsi que la collaboration entre différents pays en ce qui concerne l'application des lois dans le domaine sont essentielles pour faire échec au pourriel.

Depuis plusieurs années déjà, le Canada participe activement aux tribunes internationales consacrées à Internet. Les récentes discussions ont porté en grande partie sur les différentes mesures législatives, réglementaires et d'application prises par certains pays pour lutter contre le pourriel, ainsi que sur la nécessité de veiller à ce que les approches adoptées soient compatibles avec l'environnement mondial d'Internet.

Grâce à ces travaux, on progresse sur le front de la coordination des politiques anti-pourriel entre les pays et de la coopération internationale dans l'application des lois et règlements anti-pourriel. Certains pays y sont parvenus en greffant les mesures d'application sur les accords de collaboration en vigueur comme celui qui existe entre le Bureau de la concurrence du Canada et la Federal Trade Commission des États-Unis. Toutefois, on n'a eu recours à ces accords que dans une mesure limitée, et il faudrait en élaborer de nouveaux portant expressément sur l'application des lois et règlements anti-pourriel.

Il reste beaucoup de travail à faire pour promouvoir une coordination et une collaboration efficaces dans la lutte mondiale contre le pourriel. La coordination de la législation, de la réglementation et de leur application revêt une grande importance, mais il ne fait aucun doute à l'heure actuelle qu'une approche plus large s'impose à l'échelle internationale. De nombreux pays reconnaissent maintenant qu'une approche multiple, de type « boîte à outils », et mettant à contribution différents intervenants, approche similaire à celle que le Canada n'a cessé de préconiser, s'avère le mécanisme le plus efficace pour lutter contre le pourriel et résoudre d'autres problèmes en ligne.

Pour cette raison, le Groupe de travail sur le pourriel prône l'élaboration et l'adoption de pratiques exemplaires, afin d'assurer la coordination à l'échelle internationale de la gestion des réseaux et des entreprises de marketing par courriel. Il encourage par ailleurs les FSI, les entreprises de marketing par courriel, les utilisateurs de courriel commercial et les représentants des consommateurs canadiens à participer activement aux efforts déployés sur la scène internationale pour lutter contre le pourriel grâce à des initiatives telles que la mise en place de mécanismes d'authentification et de certification de courriel compatibles dans le monde entier.

Activités du Groupe de travail

Le Groupe de travail sur le pourriel préconise que le gouvernement du Canada et tous les intervenants canadiens participent de façon dynamique et coordonnée à l'élaboration et à la mise en œuvre d'approches bilatérales et multilatérales pour lutter contre le pourriel. À cette fin, ses membres ont pris une part active à plusieurs tribunes internationales importantes.

Collaboration multilatérale

1) Groupe de réflexion de l'Organisation de coopération et de développement économiques (OCDE)

Le Canada participe activement au Groupe de réflexion de l'OCDE sur le « spam », qui a mis au point une boîte à outils reposant sur une approche multiple similaire à celle adoptée par le Canada.

Différents pays ont proposé de diriger l'élaboration d'éléments de la boîte à outils ou d'y participer. Pour sa part, le Canada s'est porté volontaire pour effectuer une analyse comparative des cadres législatifs en place dans le monde. Il a offert également sa contribution à plusieurs autres aspects, notamment l'éducation et la sensibilisation du public, les technologies anti-pourriel ainsi que les mesures chapeautées par le secteur industriel dans la foulée des travaux du Groupe de travail canadien sur le pourriel, y compris les pratiques exemplaires que le Groupe de travail a recommandées à l'intention des FSI et des autres exploitants de réseaux.

2) Plan d'action de Londres

En octobre 2004, les représentants des secteurs public et privé de 15 pays, dont le Canada, se sont réunis à Londres, en Angleterre, pour explorer les moyens d'améliorer la collaboration internationale dans l'application des lois et règlements anti-pourriel. Comme ces différents pays possèdent différents cadres législatifs anti-pourriel, la réunion a permis de regrouper un large éventail d'organismes d'application de la loi qui ne travaillent généralement pas ensemble, notamment les organismes chargés de la protection des données et de la vie privée, de la défense des consommateurs ainsi que de la réglementation de la concurrence et des communications.

De cette réunion est sorti le Plan d'action de Londres sur la coopération internationale relative à l'application des lois anti-pourriel, qui a pour objet de trouver des moyens d'améliorer la collaboration internationale dans la lutte contre le pourriel et la résolution des problèmes connexes. Ce plan d'action ne remplace pas les accords internationaux déjà conclus entre des organismes d'application de la loi. Le but premier est plutôt d'améliorer la communication entre les différents organismes engagés dans la lutte contre le pourriel. Le Groupe de travail a indiqué qu'il appuierait le Plan d'action de Londres et, par l'intermédiaire d'Industrie Canada, il a participé à sa mise en œuvre. Le Commissariat à la protection de la vie privée du Canada y prend part également.

3) Autres mécanismes de collaboration multilatérale

Le Groupe de travail a participé aux activités de lutte contre le pourriel du Forum de coopération économique Asie-Pacifique, de l'Union internationale des télécommunications et du Sommet mondial sur la société de l'information, y compris les travaux du Groupe de travail sur la gouvernance d'Internet de l'Organisation des Nations Unies.

Le Groupe de travail sur le pourriel a également appuyé les efforts déployés dans le domaine par la Conférence des Nations Unies sur le commerce et le développement, l'Internet Engineering Task Force et le Réseau international de contrôle et de protection des consommateurs.

Par ailleurs, le Groupe de travail sur le pourriel aimerait souligner l'importance du travail que le secteur privé a effectué par l'intermédiaire d'organismes comme l'Alliance technique anti-pourriel, le Messaging Anti-Abuse Working Group et différentes associations du secteur industriel.

Initiatives bilatérales

Le Canada encourage fortement la collaboration internationale pour les besoins de l'élaboration de politiques et de stratégies anti-pourriel en vertu d'accords stratégiques bilatéraux conclus avec des partenaires clés, notamment l'Australie, le Royaume-Uni, les États-Unis, Taiwan et la Commission européenne. Des accords sont déjà conclus avec l'Australie et le Royaume-Uni, et le Groupe de travail prévoit que l'on en conclura d'autres d'ici la fin de 2005 avec les États-Unis, Taiwan et la Commission européenne.

Recommandations

Le Canada occupe depuis longtemps le rôle de chef de file international dans le domaine des politiques et des stratégies en matière de communications. Ces dernières années, son cadre stratégique global sur le commerce électronique, son marché concurrentiel des services à large bande et ses initiatives de transformation des services et de gouvernement en ligne ont retenu l'attention sur la scène internationale.

Le Groupe de travail estime que le Canada pourrait prendre les rênes de la prochaine phase de la lutte mondiale contre le pourriel. Plusieurs autres pays ont déjà adopté une loi anti-pourriel. Ils étaient les premiers à promouvoir des mécanismes d'application axés sur la collaboration, mais le Canada a affiché des résultats confirmés en ce qui touche les pratiques exemplaires du secteur industriel et sa campagne de sensibilisation du public. Il s'agit de premières étapes sûres qui démontrent l'intérêt d'adopter une approche multiple, avec différents intervenants, et suppléant par d'autres outils les lois et leur application rigoureuse.

De plus, le Groupe de travail estime que le Canada a non seulement la possibilité mais également l'obligation d'assurer le leadership international de la lutte contre le pourriel. Une des principales contributions que le pays peut apporter consiste à réduire le volume de pourriels au Canada.

En analysant l'expérience d'autres pays et les efforts déployés à l'heure actuelle pour mettre en place des mécanismes d'application axés sur la collaboration, le Groupe de travail en est arrivé aux conclusions suivantes.

- L'expérience des autres pays est riche d'enseignements quant aux moyens qui sont efficaces — et à ceux qui ne le sont pas — dans la lutte contre le pourriel et les menaces connexes auxquelles est exposé Internet. En plus de faire ressortir l'importance d'adopter une approche multiple, de type boîte à outils, et mettant à contribution différents intervenants, ces expériences témoignent de l'importance de faire reposer la lutte contre le pourriel sur des lois qui interdisent l'envoi de courriels commerciaux sans le consentement préalable des destinataires et prévoient des sanctions sévères contre les polluposteurs.
- Les mesures prises au Canada pour réduire le volume de pourriels auront une incidence limitée sur le volume de pourriels qui se retrouvent dans la boîte de réception des Canadiens, à moins qu'elles ne soient complétées et renforcées par des mesures solides et efficaces, prises en collaboration à l'échelle internationale contre les polluposteurs.
- Le Canada a la possibilité de jouer un rôle de leadership dans la lutte internationale croissante contre le pourriel, en aidant particulièrement les pays en développement à adopter une approche multiple, de type boîte à outils, et mettant à contribution différents intervenants, pour lutter contre le pourriel, et à adapter cette approche à leurs propres besoins et compétences.

En conséquence, nos recommandations sont les suivantes :

Recommandation 18 :

Le gouvernement fédéral devrait continuer de conclure avec des gouvernements étrangers des accords bilatéraux sur les politiques et les stratégies anti-pourriel.

Recommandation 19 :

Le gouvernement fédéral, en consultation, en collaboration et en partenariat avec d'autres intervenants s'il y a lieu, devrait promouvoir et appuyer de façon active la mise en œuvre coordonnée au niveau international des mesures politiques, législatives, réglementaires et d'application, des normes et pratiques du secteur industriel et des activités d'éducation et de sensibilisation du public dans le domaine de la lutte contre le pourriel.

Recommandation 20 :

Le Canada devrait mettre au service des pays en développement ses compétences dans l'élaboration d'approches multiples, de type boîte à outils, et mettant à contribution différents intervenants, pour les aider à lutter contre le pourriel.

7 COORDONNER L'ACTION FUTURE

LE DÉFI

Le succès de la mise en œuvre de la stratégie canadienne multiple regroupant divers intervenants, pour lutter contre le pourriel et les menaces connexes, exige une démarche hautement synchronisée et coordonnée en matière de prévention et d'application de la loi. Le Groupe de travail a constaté qu'une communication et une collaboration plus étroites s'imposaient dans le domaine de l'application en particulier, car il y a un grand nombre d'organismes d'application et de réglementation, et que chacun d'eux est partiellement responsable de la lutte anti-pourriel.

L'adoption de l'approche de type « boîte à outils » découle de la complexité du problème du pourriel. Celle-ci ne disparaîtra pas à la fin du mandat du Groupe de travail. On peut s'attendre, à l'avenir, à ce que le gouvernement et les autres intervenants soient confrontés à la même série de questions qui ont mené à la création du Groupe de travail. En voici quelques exemples :

- Des questions se poseront de façon continue sur l'application des lois anti-pourriel, dont celle de la coordination entre les divers organismes et compétences, celle de l'expertise technique requise pour la poursuite des enquêtes et celle de la disponibilité des ressources consacrées à la poursuite des contrevenants.
- Il faudra que les FSI et autres exploitants de réseaux continuent de partager les pratiques exemplaires et les stratégies efficaces, afin de contrer les nouvelles menaces et de mettre au point un système adéquat pour mesurer la portée du problème du pourriel au Canada et l'efficacité des mesures anti-pourriel.
- Les internautes canadiens auront un besoin constant de renseignements fiables et exacts sur les mesures à prendre pour se protéger contre le pourriel et les pratiques trompeuses, nuisibles et frauduleuses connexes. Ils auront également besoin d'un point central et d'un processus simple pour le dépôt des plaintes.
- Le besoin de coordonner la participation des intervenants canadiens dans la lutte internationale contre le pourriel sera constant et s'amplifiera.

Activités du Groupe de travail

Tenant compte de sa propre expérience et de celle des autres pays, le Groupe de travail sur le pourriel a conclu que, pour relever avec succès les défis que pose le pourriel, le gouvernement du Canada devrait établir ou désigner un point central ou centre, qui mènerait la lutte contre le pourriel et les menaces connexes. Ce centre devrait assumer deux principales fonctions : la supervision et la coordination des politiques et un appui aux organismes d'application de la loi.

Pour être un centre efficace en matière d'élaboration et de coordination des politiques, le Groupe de travail est d'avis que ce dernier devrait recevoir un mandat et des ressources lui permettant de :

- formuler des politiques visant à traiter le problème du pourriel et les menaces connexes, notamment par le suivi et l'analyse des questions et la consultation régulière des principaux intervenants;

- recueillir et compiler des renseignements et des données statistiques pour mesurer et évaluer l'ampleur du problème du pourriel au Canada et l'efficacité des mesures anti-pourriel, y compris des deux ensembles de pratiques exemplaires formulées par le Groupe de travail et les responsables de la campagne « Arrêtez le pourriel ici / Stop Spam Here »;
- fournir au public canadien les renseignements et autres ressources, ainsi que les services de soutien et d'acheminement des plaintes, dont il a besoin pour se protéger contre le pourriel;
- encourager les secteurs public, privé et universitaire à collaborer à la lutte anti-pourriel à l'échelle nationale et internationale.

Pour appuyer de façon efficace une démarche concertée à l'échelle nationale et internationale à l'égard de la lutte anti-pourriel, le Groupe de travail est d'avis que le centre devrait recevoir un mandat et des ressources lui permettant de :

- recevoir, analyser et acheminer les plaintes du public concernant le pourriel et les activités connexes;
- aiguiller les cas et les preuves à l'appui aux organismes d'application de la loi ou de réglementation appropriés;
- fournir une expertise technique à l'appui des enquêtes futures et en cours.

Le Groupe de travail a examiné quelques modèles organisationnels possibles, notamment des modèles canadiens tels PhoneBusters et le Centre national de coordination contre l'exploitation des enfants, et des modèles américains comme Operation Slam Spam et l'AntiPhishing Working Group. Cependant, il ressort de l'examen qu'aucun de ces modèles ne répondrait à toutes les exigences du double mandat qu'il a envisagé pour le centre.

Il y a essentiellement trois options possibles pour l'établissement d'un tel centre :

1) créer un nouveau partenariat public-privé à l'extérieur du gouvernement;
2) établir le centre au sein d'un ministère du gouvernement fédéral;
3) affecter les responsabilités à un organisme de réglementation existant.

Étant donné que le ministre de l'Industrie serait responsable de la loi anti-pourriel, le Groupe de travail a conclu que le centre devrait relever d'Industrie Canada. À son avis, un organisme rattaché à un ministère gouvernemental serait le plus apte à s'acquitter efficacement des fonctions de supervision des politiques ainsi que de coordination et de consultation requises.

Qui plus est, l'exploitation de la base de données sur les pourriels (le « congélateur ») et le partage de renseignements en temps réel exigera une collaboration active et constante avec le secteur privé, ce qu'un organisme ministériel pourrait sans doute faire plus facilement qu'un organisme réglementaire ou quasi-judiciaire. Le Groupe de travail tient cependant à souligner l'importance d'associer le secteur privé à l'exploitation du centre et d'inclure des représentants du secteur industriel et des consommateurs sous sa gouvernance.

Recommandations

Il est évident que dans la lutte anti-pourriel, une approche multiple, de type « boîte à outils » et regroupant divers intervenants ne fonctionnera pas à long terme à moins qu'un organisme quelconque n'ait la responsabilité, l'autorité et les ressources requises pour coordonner cette lutte.

Il est également clair que le gouvernement du Canada devra périodiquement évaluer l'ampleur de la mise en œuvre des recommandations du Groupe de travail par les intervenants, l'apport de cette démarche multiple à la réduction du pourriel et l'efficacité de la stratégie anti-pourriel du Canada pour contrer les nouvelles menaces.

En conséquence, nos recommandations sont les suivantes :

Recommandation 21 :

Afin de poursuivre la démarche multiple, de type « boîte à outils » et regroupant divers intervenants formulée par le Groupe de travail sur le pourriel et de fournir un point central pour faciliter la mise en œuvre de ses recommandations, le gouvernement devrait établir un centre relevant du ministre de l'Industrie, qui assumerait la supervision et la coordination des politiques, l'éducation et la sensibilisation du public et fournirait un appui aux organismes d'application des lois.

Recommandation 22 :

Le gouvernement fédéral, par le truchement de cet organisme de coordination, devrait surveiller les répercussions de la mise en œuvre des recommandations du Groupe de travail, évaluer les résultats, faire rapport régulièrement au public et, en consultation avec les intervenants, prendre toutes les mesures supplémentaires requises pour lutter contre le pourriel.

APPENDICES

APPENDICE A

MEMBRES DES SOUS-GROUPES DU GROUPE DE TRAVAIL ET SECRÉTARIAT

La législation et son application

Coprésidents

Michael Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Université d'Ottawa
Roger Tassé, associé, Gowlings Lafleur Henderson s.r.l.

Organisations membres

Amazon.com
Association canadienne de la technologie de l'information
Association canadienne des télécommunications par câble
Association canadienne des télécommunications sans fil
Bell Canada
Bureau de la concurrence
Bureau de la consommation, Industrie Canada
Clinique d'intérêt public et de politique d'Internet du Canada
Coalition canadienne contre le pourriel
Cogeco Câble inc.
Commissariat à la protection de la vie privée du Canada
Conseil de la radiodiffusion et des télécommunications canadiennes
First Data Corporation
Gendarmerie royale du Canada
LinuxMagic
Microsoft Canada
Ministère de la Justice du Canada
Nortel Networks
PayPal Inc.
Rogers Communications Inc.
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada
TELUS Communications Inc.

Technologies et gestion de réseaux

Coprésidents

Tom Copeland, président, Association canadienne des fournisseurs Internet
Lori Assheton-Smith, première vice-présidente et avocate, Association canadienne de télévision par câble

Organisations membres

Agence canadienne d'enregistrement Internet
Allstream
AOL Canada
Association canadienne des télécommunications sans fil
Bell Canada
BorderWare Technologies Inc.
CANARIE Inc.
CipherTrust
Coalition canadienne contre le pourriel
Cogeco Câble inc.
Delta Cable Communications
easyDNS Technologies Inc.
E-Gate Communications Inc.
Groupe Télécom
Interlink Connectivity
Internet Light and Power
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
LinuxMagic
MessageLabs Americas
Microsoft Canada
Nortel Networks
PhoneBusters
Rogers Communications Inc.
Secteur de l'agent principal de l'information, Industrie Canada
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada
SecuritySage Inc.
Shaw Communications Inc.
Spamhaus
TELUS Communications Inc.
Université de la Colombie-Britannique
Université du Manitoba
Vidéotron Télécom ltée
Vircom inc.

Validation du courriel commercial

Coprésidents

Neil Schwartzman, président, Coalition canadienne contre le pourriel
Amanda Maltby, première vice-présidente, Relations publiques Ipsos-Reid, représentant l'Association canadienne du marketing

Organisations membres

24/7 Canada Inc.
AOL Canada
Association canadienne de la technologie de l'information
Association canadienne des télécommunications par câble
Association canadienne du marketing
Bell Canada
Bureau de la consommation, Industrie Canada
Conseil consultatif canadien sur les normes de TIC
Cornerstone Group of Companies
Daemon Defense Systems
Digital Cement
Doubleclick
eBay Inc.
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
MS Planners
Partners Inc.
Rogers Communications Inc.
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada
Technology Surveys International

Éducation et sensibilisation du public

Coprésidents

Suzanne Morin, première conseillère juridique, affaires juridiques et questions de réglementation, Bell Canada
Geneviève Reed, responsable du Service de recherche et de représentation, Option consommateurs

Organisations membres

Association canadienne de la technologie de l'information
Association canadienne des fournisseurs Internet
Bell Canada
Bureau de la concurrence
Bureau de la consommation, Industrie Canada
Centre pour la défense de l'intérêt public
Chambre de commerce du Canada
Clinique d'intérêt public et de politique d'Internet du Canada
Coalition canadienne contre le pourriel
Commissariat à la protection de la vie privée du Canada
Conseil des consommateurs du Canada
Openface Internet Inc.
Réseau Éducation-Médias
Secteur de l'agent principal de l'information, Industrie Canada
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada
Union des consommateurs

Collaboration internationale

Coprésidents

Bernard Courtois, président, Association canadienne de la technologie de l'information
Michael Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Université d'Ottawa

Organisations membres

Bell Canada
Bureau de la concurrence
Chambre de commerce du Canada
Commission européenne
LinuxMagic
Microsoft Canada
Ministère des Communications, de la Technologie de l'information et des Arts d'Australie
Ministère du Commerce et de l'Industrie du Royaume-Uni
Organisation de coopération et de développement économiques
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada

Secrétariat du Groupe de travail

Secteur du Spectre, des technologies de l'information et des télécommunications, Industrie Canada

Richard Simpson, directeur général, Direction générale sur le commerce électronique
Shari Scott, directrice, Direction générale sur le commerce électronique
David Charter, Direction générale sur le commerce électronique
Gérard Desroches, Direction générale sur le commerce électronique
Peter Ferguson, Direction générale sur le commerce électronique
Lisa Foley, Direction générale sur le commerce électronique
Angie Forte, Direction générale sur le commerce électronique
Jennifer Kealey, Direction générale sur le commerce électronique
Serge Presseau, Direction générale sur le commerce électronique
Howard Chatterton, Services techniques d'homologation et de télécommunications
David Gibson, Services techniques d'homologation et de télécommunications

Don MacLean, auteur du rapport, MacLean Consulting
John Levine, auteur du glossaire et réviseur technique

APPENDICE B

PRATIQUES EXEMPLAIRES RECOMMANDÉES POUR LES FOURNISSEURS DE SERVICE INTERNET ET LES AUTRES EXPLOITANTS DE RÉSEAUX

Contexte

En août 2004, le Sous-groupe sur les technologies et la gestion de réseaux a entrepris l'élaboration d'un certain nombre de pratiques exemplaires techniques qui contribueraient à réduire le volume de pourriel. Son mandat s'inscrit dans la foulée des efforts et des progrès accomplis depuis quelque temps au Canada et à l'échelle internationale, dont les travaux de l'Anti-Spam Technical Alliance (ASTA) et du Messaging Anti-Abuse Working Group (MAAWG), ainsi que ceux de plusieurs associations du secteur d'activités. Un certain nombre de fournisseurs de service Internet (FSI), d'autres exploitants de réseaux et des groupes techniques collaborent depuis de nombreux mois afin de partager leurs pratiques exemplaires pour réduire le pourriel.

Le Sous-groupe n'a pas essayé de refaire le travail déjà accompli, préférant réunir les divers groupes du secteur industriel pour mettre en commun les résultats du travail en cours et encourager l'adoption des pratiques exemplaires par les FSI, les autres exploitants de réseaux et les grandes entreprises qui utilisent Internet.

Le Sous-groupe tient à souligner que l'adoption répandue de ces pratiques ne constituera pas à elle seule une solution exhaustive au problème du pourriel. Toutefois, les recommandations font partie d'une stratégie à facettes multiples plus vaste visant à le régler.

Intention

Les pratiques exemplaires en matière de lutte anti-pourriel recommandées au secteur industriel par le Sous-groupe sont volontaires. L'échéancier de leur mise en œuvre peut varier selon la configuration technique particulière du réseau du fournisseur de service ou de l'exploitant ainsi que des besoins et de la situation de celui-ci. Dans certains cas, des solutions de rechange peuvent permettre d'atteindre les mêmes objectifs que ceux des recommandations. Le choix des solutions reste à la discrétion du fournisseur de service ou de l'exploitant de réseau.

Le Sous-groupe appuie tous les efforts déployés pour combattre le pourriel. La souplesse inhérente à la mise en œuvre de ces pratiques exemplaires est l'élément essentiel à une adoption généralisée et efficace par les fournisseurs de service de toutes tailles. Vu la nature technique de ces recommandations et l'évolution rapide de la technologie, le Sous-groupe est persuadé qu'il faut éviter de codifier ces pratiques exemplaires sous forme d'exigences obligatoires.

Pratiques exemplaires recommandées et leurs fondements

Pratiques exemplaires recommandées pour les fournisseurs canadiens de service Internet et les autres exploitants de réseaux pour lutter contre le pourriel, et les fondements pour chacune des recommandations.

1. Tous les registraires et hôtes canadiens de noms de domaine devraient publier des renseignements sur Sender Policy Framework (SPF) dans les fichiers de leur zone respective de serveur de nom de domaine le plus tôt possible.

Le but de l'authentification de l'expéditeur de courriel est de réduire la mystification du nom de domaine dans le courriel, réduisant par le fait même la fréquence des tentatives de pourriel et d'hameçonnage.

Le groupe Internet Engineering Task Force (IETF) continue d'évaluer les méthodes d'authentification de l'expéditeur de courriel. À l'heure actuelle, la proposition relative au SPF classique (SPFv1) est le modèle de conception d'authentification de l'expéditeur de courriel le plus techniquement avancé et le plus largement déployé.

Cette recommandation n'empêche pas l'utilisation d'autres propositions qui authentifieront des courriels (par exemple Sender-ID, Domain Keys, SPF, courrier Internet identifié, etc.). Le secteur industriel continuera d'élaborer des normes à cet égard.

2. Les FSI et autres exploitants de réseaux devraient limiter, par défaut, l'utilisation du port 25 par les utilisateurs finaux. Au besoin, la capacité d'envoyer ou de recevoir du courriel au moyen du port 25 devrait être limitée aux ordinateurs hôtes du réseau du fournisseur. L'utilisation du port 25 par les utilisateurs finaux devrait être permise au besoin ou être conforme à l'entente entre le fournisseur et l'utilisateur final et aux modalités de service.

Selon la majorité des FSI et autres exploitants de réseaux, il n'y a aucune raison pratique pour que des utilisateurs clients aient des serveurs de courrier utilisant des intervalles d'adresses Protocole Internet (IP) commutées/dynamiques.

Il y a plusieurs façons d'éliminer ce problème. Les FSI et autres exploitants de réseaux peuvent se servir de leur propre outil de gestion de réseau pour bloquer la sortie de messages par le port 25.

D'après leur expérience, les membres de ce sous-groupe savent que le blocage du port 25 n'affecte qu'un très petit nombre d'utilisateurs et que ces derniers peuvent normalement s'accommoder de façons différentes.

Les avantages de ce blocage peuvent être énormes. Ainsi, des FSI ont constaté une diminution de 95 p. 100 des émissions de virus, de 98 p. 100 des rapports d'abus et une réduction des infections internes de virus et des appareils infectés servant à envoyer des pourriels, ajoutant à cela la réduction des coûts reliés à la gestion des abus de réseau.

3. Les FSI et autres exploitants de réseaux devraient filtrer les pièces jointes aux courriels dont les extensions sont connues pour transporter des virus ou filtrer les pièces jointes en fonction des propriétés du contenu.

Un grand nombre de virus et de vers sont acheminés par les pièces jointes. Le blocage des courriels contenant des pièces jointes problématiques aurait peu de répercussions sur les utilisateurs. Les extensions de fichiers les plus susceptibles de porter des virus sont : .pif, .scr, .exe et .vbs.

Bon nombre de FSI et autres exploitants de réseaux devraient filtrer les pièces jointes en fonction des propriétés (c'est-à-dire des infections) par opposition aux noms d'extension. C'est une question de disponibilité des ressources. Étant donné que certains utilisateurs commerciaux et techniques pourraient avoir des motifs valables d'envoyer des fichiers comportant des extensions .exe ou .vbs, il se peut que le filtrage du contenu soit plus efficace que celui des noms d'extension.

4. **Les FSI et autres exploitants de réseaux devraient surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence.**

La surveillance et la limitation éventuelle de la quantité de courriels qu'un utilisateur donné pourrait envoyer décourageraient les polluposteurs d'utiliser les réseaux des fournisseurs comme point d'envoi. Ces mesures serviraient également de premier indice d'infection de l'appareil d'un utilisateur.

Actuellement, certains fournisseurs se restreignent quant à la limitation de la quantité de courriels expédiés. Les techniques varient en fonction du serveur de courriel utilisé.

5. **Les FSI et autres exploitants de réseaux devraient établir et maintenir de façon continue des processus efficaces et rapides pour la gestion et l'élimination des éléments de réseau infectés constituant une source de pourriel.**

Au moyen de virus, de programmes-vers et de logiciels pernicieux, les pirates informaticiens et polluposteurs ont délibérément installé des millions de relais ouverts de type « porte arrière » et de passerelles de procuration sur les ordinateurs personnels d'utilisateurs peu méfiants. Les polluposteurs utilisent ce réseau d'appareils infectés pour générer des milliards de courriels non sollicités. En plus, les pirates ont utilisé ce réseau d'appareils informatiques à des fins d'exécution de Refus de service distribué sur les sites Web, d'inscription de comptes frauduleux et de préparation à des activités anonymes futures de piratage informatique.

Diverses méthodes peuvent être utilisées pour traiter les appareils infectés, notamment la suspension de comptes-clients, l'isolement ou la mise en quarantaine de ces appareils à l'extérieur du réseau.

6. **Les FSI et autres exploitants de réseaux devraient établir des processus interentreprises pertinents afin de réagir aux rapports d'incidents des autres exploitants de réseaux.**

Le Sous-groupe sur les technologies et la gestion de réseaux dresse présentement une liste de personnes-ressources des FSI et autres exploitants. Il serait utile de pouvoir s'attendre à une réponse commune lorsqu'on signale un incident d'abus de réseau important à un autre opérateur de réseau. Le processus de recours hiérarchique au sein des entreprises demeurerait un processus privé, mais une « heure de reprise prévue commune » devrait figurer dans les communications initiales interentreprises.

7. **Les FSI et autres exploitants de réseaux ainsi que les fournisseurs de service de courrier électronique devraient communiquer leurs politiques et procédures en matière de sécurité à leurs abonnés.**

Ce point vise à faire en sorte que les abonnés soient bien au courant des politiques et procédures de sécurité de leur FSI, des autres exploitants de réseaux et des entreprises fournissant des services de courriel. Ce point aura une importance particulière pour les recommandations 2, 3 et 5.

Un autre sous-groupe du Groupe de travail, celui sur l'éducation et la sensibilisation du public, a élaboré une campagne multilatérale d'information et de sensibilisation du public afin de faire connaitre, particulièrement aux utilisateurs finaux canadiens, les méthodes à prendre pour limiter la quantité de courriels commerciaux non sollicités reçus.

8. Les FSI et autres exploitants de réseaux devraient adopter la validation du courriel sur tous leurs serveurs Simple Mail Transfer Protocol (SMTP) (c'est-à-dire entrée, sortie, relais).

La validation du courriel ferait en sorte que seuls les clients « authentifiés » seraient autorisés à envoyer du courrier sur le serveur. Par exemple, l'authentification SMTP est une amélioration qui permet aux serveurs SMTP de vérifier l'identité des clients du système de courriel. Le protocole demande le nom d'utilisateur et le mot de passe de l'expéditeur du message et les valide en les comparant aux données des clients préinscrits. Cette procédure peut être utilisée pour réduire les pourriels, car ceux-ci ne proviennent généralement pas d'utilisateurs inscrits sur la liste d'autorisation SMTP.

9. Les avis de non-remise (NDN) ne devraient être envoyés que dans les cas de courriels légitimes.

Les gestionnaires d'Agents de transfert des messages (ATM) et les fabricants de filtres anti-pourriel ont maintenant accepté cette pratique. Quand un message est envoyé à un compte d'utilisateur non existant, l'ATM répond que l'utilisateur n'existe pas. Cela peut causer des problèmes lorsqu'un polluposteur contrefait un grand nombre d'adresses d'un domaine, car le serveur émet une réponse de non-remise pour chaque adresse non existante. Le logiciel ATM devrait être configuré de manière à ne pas envoyer de messages de non-remise dans les cas d'adresses contrefaites.

La cessation généralisée des NDN pourrait causer des problèmes aux utilisateurs qui ont mal tapé l'adresse et présument que le message est parvenu au destinataire.

10. Les FSI et autres exploitants de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers de systèmes de noms de domaine (DNS) et les fichiers d'enregistrement d'adresse IP applicables (WHOIS/SWIP/RWHOIS) soient maintenus à jour à l'aide de renseignements corrects, complets et courants. Ces renseignements devraient comprendre les points de contact responsables de résoudre les questions d'abus et inclure, sans toutefois s'y limiter, les adresses postales, les numéros de téléphone et les adresses de courriel.

L'identification de points de contact pour les FSI et les exploitants de réseaux est essentielle à la gestion des abus des systèmes de communication électronique. Tous les courriels comprennent des renseignements tels que les noms Internet DNS, les adresses IP et autres données concernant la source, la transmission et la destination du message. Les FSI et autres exploitants de réseaux responsables des sources des courriels devraient être facilement et exactement identifiables. Les noms de domaine qualifiés (par exemple nomInternet.nomdedomaine.ca), les noms de domaine et les adresses IP devraient être enregistrés et maintenus à l'aide de renseignements permettant cette identification.

Les exploitants de réseaux devraient également voir à ce que les fichiers de nom de domaine, les fichiers DNS avant et inversés et les fichiers de la base de données WHOIS, du projet partagé WHOIS (c'est-à-dire SWIP) ou de référence (c'est-à-dire RWHOIS) soient adéquatement maintenus à l'aide de données exactes, complètes et courantes. Par exemple, les fichiers WHOIS de l'American Registry for Internet Numbers devraient inclure OrgAbuseHandle, y compris les coordonnées des responsables de la gestion des abus provenant de ce réseau. Les FSI et les exploitants de réseaux sont responsables du maintien de données d'enregistrement, de fichiers DNS et autres renseignements signalétiques conformes aux documents Request for Comments (RFC) pertinents, notamment le RFC 2142 — Mailbox Names for Common Services, Roles and Functions.

11. Les FSI et autres exploitants de réseaux devraient veiller à ce que leurs adresses routables publiques et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP. Tous les exploitants de réseau local d'entreprise (RLE) devraient se conformer au document Request for Comments (RFC) 1918 — « Address Allocation for Private Internets ». Les RLE, plus particulièrement, ne devraient pas utiliser l'espace IP enregistré globalement à quelqu'un d'autre ou l'espace IP non enregistré à quelqu'un, à titre d'espace IP privé.

Le pourriel et le maliciel comportent souvent un en-tête de courriel contrefait. Il importe donc de veiller à ce que toutes les adresses routables publiques et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP, afin de pouvoir repérer les sources des courriels et autres modes de communication en ligne. L'identification de la source permet d'avertir les FSI ou les autres exploitants de réseaux responsables afin qu'ils puissent prendre des mesures appropriées pour éliminer le pourriel ou les autres problèmes associés au protocole. Les adresses IP enregistrées auprès d'un autre organisme ne devraient pas être utilisées au sein des réseaux privés, car elles entravent considérablement l'identification des FSI et autres exploitants de réseaux responsables d'un courriel. Les destinataires peuvent utiliser les noms Internet DNS à des fins de politique d'accès, mais les noms doivent être soigneusement choisis, afin d'éviter que des filtres trop vastes ne bloquent les courriels légitimes. Prière de consulter la recommandation 10 concernant le maintien des fichiers à l'aide de renseignements exacts, complets et courants.

Pour faciliter l'identification des sources de courriels, on suggère également que les serveurs aient des noms Internet DNS qui différencient clairement ces serveurs des adresses des postes de travail des consommateurs ou des entreprises. Les noms Internet des fichiers DNS avant (traduction de l'adresse IP en nom Internet) et inversés (traduction du nom Internet en adresse IP) devraient correspondre. Les clients des FSI autorisés à exploiter des serveurs de courriel ou autres serveurs profiteront de cela, car ils pourront exploiter des systèmes DNS avant et inversés au sein de leur domaine, distinguant ainsi les hôtes des hôtes résidentiels ou des hôtes interdits. Les destinataires de courriels peuvent ainsi établir des systèmes qui différencient les serveurs de courriel légitimes des hôtes susceptibles d'être des sources de pourriel.

Les adresses IP résidentielles, dynamiques ou interdites devraient également prévoir une convention d'adressage par domaines avant et inversé claire et uniforme. Par exemple, les politiques de contrôle d'accès des destinataires qui distinguent les sources de courriel fiables des sources non fiables sont plus faciles à établir lorsque les conventions d'adressage incluent le propriétaire du domaine, la classe de service, l'affectation statique ou dynamique et d'autres identificateurs, notamment une identification axée sur une fourchette d'adresses IP. Ces conventions peuvent également empêcher que les clients des FSI autorisés à exploiter des serveurs de courriel soient bloqués parce qu'il est impossible de les distinguer des sources de courriels illégitimes. Les conventions d'adressage comportant un schéma « de plus fort poids à droite » simplifient les filtres et font en sorte que les politiques de contrôle d'accès n'affectent pas les sources de courriels légitimes. Par exemple, une telle convention d'adressage pour l'adresse IP résidentielle, dynamique « 1.2.3.4 » au FSI Example.ca serait « 4-3-2-1.dyn.res.example.ca. ». Un exemple de convention d'adressage pour l'adresse IP commerciale, statique « 1.2.3.4 » au FSI Example.ca serait « 4-3-2-1.static.bus.example.ca. ». Un exemple de convention d'adressage pour un serveur de courriel utilisé par Smallbizcustomer.ca serait « mail.smallbizcustomer.ca ».

12. **Les FSI et autres exploitants de réseaux devraient interdire l'envoi de courriels renfermant des en-têtes frauduleux ou contrefaits. L'en-tête de message devrait être exact et conforme aux documents RFC pertinents, notamment le RFC 822 et le RFC 2822, et les domaines de référence et les adresses IP devraient comporter des données d'enregistrement exactes et à jour.**

Un en-tête de courriel exact permet aux FSI et aux autres exploitants de réseaux de repérer les sources de pourriel et de maliciel électronique au sein de leur réseau FSI. Prière de consulter la recommandation 10 concernant le maintien des fichiers à l'aide de renseignements exacts, complets et courants.

Bien que les réseaux internes utilisent souvent des adresses IP privées (conformément au document RFC 1918 — Address Allocation for Private Internets) qui ne sont pas routables ni identifiables extérieurement, les fournisseurs de service de courriel devraient s'assurer que les sources de courriels sont correctement identifiables à des fins d'application des politiques et des lois.

Conclusion

Le pourriel est un problème global et multiple, exigeant l'adoption de mesures concertées à plusieurs niveaux afin d'arriver à des résultats réels et mesurables. La mise en œuvre des recommandations présentées dans ce document peut aider à réduire un grand nombre des pires formes de pourriel, de contrefaçon et d'usurpation d'identité que l'on retrouve dans les courriels. À défaut de mettre fin au pourriel, ces mesures amélioreront grandement la capacité de la communauté Internet d'en repérer la source et de tenir les expéditeurs responsables de leurs gestes. Ces mesures devraient également servir de base aux solutions futures.

APPENDICE C

PRATIQUES EXEMPLAIRES RECOMMANDÉES POUR LE MARKETING PAR COURRIEL

Contexte

Le Groupe de travail sur le pourriel du gouvernement fédéral a mis sur pied le Sous-groupe sur la validation du courriel commercial chargé d'élaborer une série de pratiques exemplaires pour le marketing par courriel. Ces pratiques exemplaires encourageront les organismes canadiens à adopter des techniques de marketing anti-pourriel et renforceront le fait que le pourriel n'a aucun rôle légitime à jouer dans le marketing canadien.

La majorité des organismes responsables respectent déjà les codes du secteur industriel ou ont adopté des pratiques exemplaires. Au Canada, les organismes observent le *Code de déontologie et les Normes de pratiques* de l'Association canadienne du marketing. Ce document renferme des lignes directrices s'appliquant au marketing par courriel et à la collecte en ligne de données pour le marketing. Les membres des organismes faisant partie du Conseil canadien de la recherche par sondage, qui mènent des sondages en ligne, sont également en train d'élaborer un code de pratique uniforme.

Le présent document regroupe une liste de pratiques exemplaires fondées sur les codes actuels, destinées à servir de fondement à l'usage du courriel à des fins commerciales ou de marketing.

Les fournisseurs de services Internet et les fournisseurs de services de courriel utilisent de plus en plus souvent les filtres et les listes blanches et noires pour bloquer le pourriel, mais ce faisant, ils empêchent les courriels légitimes d'atteindre leurs destinataires. Les organismes sont encouragés à adopter les pratiques exemplaires énoncées ci-dessous pour s'assurer que leurs courriels légitimes atteignent les destinataires prévus.

Ces pratiques exemplaires ne sont pas juridiquement contraignantes, mais elles sont un complément aux lois canadiennes actuelles régissant le pourriel, la protection des renseignements personnels, le marketing par courriel et le marketing auprès des enfants. À titre d'exemple, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), entrée en vigueur au Canada en janvier 2004, énonce les obligations des personnes qui recueillent, utilisent et communiquent les adresses de courriel personnelles. D'autres lois fédérales, notamment la *Loi sur la concurrence*, la *Loi sur les télécommunications* et le *Code criminel*, sont pertinentes. Les organismes devraient se familiariser avec ces lois et régir leurs activités en conséquence.

Les pratiques exemplaires, accompagnées de notes explicatives et d'exemples, sont décrites dans les pages suivantes.

Pratiques exemplaires recommandées

1. Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.

Cette pratique exemplaire est directement liée à l'envoi de courriels commerciaux non sollicités pour offrir des biens ou des services. Les organismes qui n'ont pas obtenu le consentement explicite des destinataires avant d'envoyer ce type de courriels envoient du pourriel.

Un organisme peut, pour ses relations d'affaires existantes (voir le glossaire), se fier au consentement implicite. En vertu de la loi canadienne actuelle, l'organisme possède le consentement implicite d'une personne pour lui envoyer un courriel lorsque celle-ci a participé à un concours, a fait un don, s'est enregistrée en ligne pour obtenir un produit ou un bulletin; a fourni son adresse de courriel suite à

une transaction; avait l'option de se retirer de l'envoi de futurs courriels mais a omis de le faire. En utilisant cette forme de consentement, l'entreprise de marketing devrait expliquer au destinaire visé pourquoi il reçoit le courriel en question. Au cours des communications de suivi, l'organisme devra fournir au destinataire l'option de se retirer de l'envoi futur de courriels de marketing (voir la pratique exemplaire 2).

Les organismes ne devraient pas envoyer des courriels de marketing aux destinataires qui ont indiqué qu'ils ne voulaient pas recevoir de courriels de leur part. Bien qu'un organisme puisse envoyer des courriels durant une relation commerciale active, il doit en tout temps respecter la volonté des personnes qui ont demandé d'être retirées des listes d'envoi de courriels de marketing. L'inclusion d'une option de retrait dans chaque message envoyé peut servir à cette fin (voir la pratique exemplaire 2).

L'envoi de courriels en dehors d'une relation d'affaires courante, ou si le dossier d'un client est devenu inactif, est justifié uniquement si l'organisme a des renseignements sur le service, la garantie ou la mise à jour d'un produit ou si l'achat d'un produit soulève des questions de santé et de sécurité. Cependant, il doit agir avec discrétion car toute tentative de vente de gamme supérieure ou de vente croisée pourrait porter ses clients à considérer le message comme du pourriel.

2. Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.

Tous les courriels envoyés aux clients doivent comporter une option de retrait. Cette option ne doit pas être cachée dans le courriel et doit, au minimum, être accessible dans un site Web ou par courriel. Le message devrait être aussi simple que celui-ci : « Si vous ne voulez plus recevoir d'offres promotionnelles de cet organisme, veuillez **cliquer ici** ou envoyer un courriel à **info@societeABC.com**. »

La procédure de retrait devrait être simple et explicite, et les organismes devraient confirmer par courriel que le retrait est ou sera respecté sans nouvelle démarche de la part du consommateur.

Au Canada, la pratique exemplaire du secteur industriel relativement aux fichiers téléphoniques ou de courrier « ne pas contacter » énonce que les demandes de retrait sont respectées pendant trois ans. Après ce délai, les organismes peuvent recommencer à présenter des offres de marketing aux particuliers. Cependant, à cause de la nature sensible des communications par courriel et des problèmes dus au pourriel, les organismes devraient considérer une demande de retrait comme finale et retirer le demandeur de leurs listes de marketing jusqu'à ce que celui-ci exprime sa volonté de recommencer à recevoir des courriels.

3. Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.

Les organismes devraient s'assurer qu'ils ont les moyens de respecter les demandes de retrait en temps voulu et mettre leurs listes à jour en conséquence.

De plus, les organismes devraient mettre en place une procédure interne d'enregistrement des preuves de consentement, notamment la date, l'heure, l'adresse de protocole Internet (IP) d'origine et l'emplacement (y compris l'URL) où l'adresse a été recueillie ainsi que le mode d'obtention du consentement s'il est différent (par exemple, carte d'affaires, formulaire de concours, téléphone, communication verbale ou carte de crédit [par exemple, par l'entremise d'un abonnement payant à une liste]). Les organismes devraient pouvoir fournir ces renseignements à un destinataire sur demande.

4. Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.

Le nom de l'expéditeur et la source du courriel devraient être clairement indiqués et mis en évidence et, dans la mesure du possible, placés au-dessus du pli (partie du courriel visible sans défilement).

Exemple 1 : Courriel envoyé directement d'un organisme à un abonné

> Date : mardi, 5 oct. 2004 07:32:02 –0400
> De : Bell Canada – Facture électronique <facture.presentation@bell.ca>
> À : JOE CONSOMMATEUR <joe@consommateur.ca>
> Objet : Votre facture électronique Bell est prête / Your Bell e-bill is ready

Exemple 2 : Courriel d'un tiers fournisseur de courriel au nom d'un organisme

> De : PUBLICATIONS peteMOSS <bounces@peteMOSS.com>
> <v2user-13990-IXoyuP..CahrNet_0bkttg@mailer.whitehat.com>
> Sujet : spamNews 07/21/04
> À : <joe@consommateur.ca>
> Date : Sam. 24 juil. 2004 18:50:17 -0700

Même si le contenu correspond à la ligne de mention objet, les organismes doivent éviter d'utiliser les termes « offres gratuites » ou « prix à gagner » et ce, parce que certains filtres anti-pourriel utilisent ce genre de mot-clé pour signaler un pourriel.

Les courriels devraient inclure l'adresse postale principale de l'expéditeur. Les organismes canadiens sont fortement encouragés à se familiariser avec les dispositions des lois canadiennes à ce sujet et les lois connexes des autres compétences, notamment de l'Australie, des États-Unis et de l'Union européenne.

5. Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'usager ou d'autres techniques de surveillance des sites Web.

En vertu de la LPRPDE, les organismes doivent faire preuve de beaucoup de transparence lorsqu'ils communiquent leurs pratiques de collecte et de traitement des renseignements personnels. Une politique sur la protection des renseignements personnels pourrait articuler la politique de l'organisme concernant le genre de renseignements recueillis et/ou utilisés, la communication des renseignements à des tiers, l'usage de mouchards (« cookies », en anglais) ou autres mesures passives de collecte de données et les procédures de sécurité, de responsabilité et d'application.

Les organismes doivent afficher leur politique complète sur la protection des renseignements personnels bien en évidence sur leur site Web, laquelle explique leurs procédures à l'égard de la collecte de renseignements en ligne. La politique devrait également inclure un lien actif vers un mécanisme d'option de retrait.

6. Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.

Les organismes, les courtiers et les propriétaires de listes d'adresses devraient assumer la responsabilité conjointe des envois de courriels aux destinataires qui n'ont pas fourni un consentement approprié. L'organisme, le courtier ou le propriétaire de listes d'adresses qui sait ou aurait dû savoir que le consentement approprié n'a pas été obtenu devrait être tenu responsable. Voici quelques mesures raisonnables qu'un organisme peut adopter pour s'assurer que ses listes sont correctes :

- consulter la politique en matière de protection des renseignements personnels du courtier ou propriétaire de la liste;
- examiner les procédures d'inclusion utilisées pour obtenir les adresses de courriel;
- demander au courtier ou au propriétaire de signer un contrat garantissant qu'il s'est conformé aux exigences de la LPRPDE (voir l'exemple de lettre à la fin du présent appendice).

7. **Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.**

Les organismes devraient consulter les Considérations spéciales se rapportant au marketing destiné aux enfants et aux adolescents, énoncées dans le *Code de déontologie et les Normes de pratiques* de l'Association canadienne du marketing (**www.the-cma.org/consumer/ethics.cfm**), ainsi qu'aux lois canadiennes (voir **www.justice.gc.ca**) pour obtenir des directives.

La façon dont les mineurs perçoivent les courriels de marketing et y réagissent est fonction de leur âge, de leur expérience et du contexte du message. Par exemple, le marketing approprié aux adolescents ne convient pas nécessairement aux enfants. En outre, on ne peut savoir avec certitude l'âge d'une personne qui s'inscrit à une liste de diffusion de courriels. Par conséquent, les organismes devraient faire preuve de discrétion et de sensibilité lorsqu'ils font du marketing auprès des mineurs et tenter d'obtenir l'autorisation des parents pour envoyer ce type de communication.

8. a) **Lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu.**

Le contenu destiné aux adultes inclut le matériel de nature sexuellement explicite et le matériel portant sur les jeux de hasard, le tabac, l'alcool, les armes à feu et autres armes.

b) **Tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.**

On pourrait demander par exemple au récipiendaire de fournir un numéro de téléphone pour que l'organisme puisse vérifier s'il a l'âge de la majorité. Il importe de noter que les contrats mettant en cause des mineurs ne sont pas applicables.

9. **Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.**

Toutes les plaintes des particuliers concernant l'usage de leur adresse de courriel devraient être traitées avec courtoisie et dans un délai raisonnable.

10. **Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :**

a) ils ont obtenu leur consentement;

b) ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou à la prestation de services associés à cet achat);

c) les destinataires savent pourquoi ils reçoivent des courriels;

d) il y a un moyen facile de refuser de recevoir davantage de courriels.

Les organismes peuvent divulguer l'adresse de courriel de leurs clients à un tiers affilié ou au sein d'une famille de sociétés à des fins de marketing croisé seulement s'ils offrent à ces clients un moyen facile de refuser de recevoir d'autres courriels de marketing avant de divulguer leur adresse de courriel.

Le motif des offres de marketing additionnelles reliées (par exemple portant la marque d'une société) devrait être évident pour les clients. L'organisme ne devrait pas présumer que les clients comprennent une relation ou une structure organisationnelle.

Pour obtenir d'autres directives, les organismes sont encouragés à consulter les pratiques exemplaires énoncées dans le *Code de déontologie et Normes de pratique*, à la section E4.1.3 du *Guide de conformité de l'ACM sur les communications de marketing électroniques*, de l'Association canadienne du marketing (ACM). La section énonce qu'une entreprise ne peut divulguer l'adresse de courriel d'un particulier à une tierce partie (par exemple société de location de listes) sans d'abord obtenir le consentement explicite (ou demande d'adhésion ou consentement positif) du particulier. Pour divulguer des adresses de courriel à des partenaires de marketing ou à des courtiers de listes d'adresses, la société doit obtenir un consentement positif. De même, elle doit obtenir une autorisation appropriée pour utiliser les adresses de courriel qu'elle a obtenues d'autres parties.

L'ACM définit le terme « tierces parties » comme suit :

> « Le terme "tierce partie" fait référence à un organisme distinct de celui avec lequel le client a originellement fait affaire (société de location de listes), y compris un organisme associé à l'organisme original (ou société de bienfaisance) ou faisant partie du groupe, mais dont la relation n'est pas évidente pour le client. Les tiers ne comprennent pas les organismes de traitement des données agissant au nom de l'organisme avec lequel le particulier a établi une relation d'affaires. »

Conseils techniques pour les entreprises de marketing électronique

1. **Les expéditeurs devraient mettre en œuvre les spécifications techniques standard suivantes :**

- Tous les serveurs (par exemple entrée, sortie, sites Web) doivent avoir des pointeurs de système de noms de domaine (DNS) inverse — rDNS PTR — dans les fichiers DNS; les outils de recherche avant et inverse de l'hôte doivent correspondre et les appareils d'envoi doivent utiliser ce nom pour la commande HELO/EHLO.
- Les fichiers Sender Policy Framework (SPF) (par exemple **http://spf.pobox.com**) et clef de domaine (domain-key) (par exemple **http://antispam.yahoo.com/domainkeys**) devraient être publiés par les expéditeurs et les sites tierces parties associés à un envoi (par exemple sites Web, processeurs de services prolongés, etc.) et tenus à jour en tout temps. On devrait envisager l'adoption de technologies semblables à mesure qu'elles sont mises au point et sont normalisées.
- Les adresses IP distinctes des autres serveurs de site devraient être assignées aux serveurs de courriel sortant.
- Les fichiers des domaines d'expéditeur de la base de données WHOIS doivent toujours être exacts et complets.
- Les noms de famille (par exemple postmaster@ et abuse@) doivent être fonctionnels et activement surveillés pour tous les domaines d'expéditeur, y compris les sites Web, mentionnés dans le contenu du courriel.

2. Les expéditeurs doivent traiter les messages de non-livraison comme suit :

- Ils doivent promptement retirer les adresses « hard » générant un message de non-livraison permanente (5xx : Utilisateur non existant / boîte aux lettres non disponible, etc.) des listes qu'ils contrôlent lorsque le nombre total de refus excède 3, en 14 jours. Si une non-livraison permanente indique un blocage de pourriel, ils peuvent réactiver l'adresse en retirant le blocage de pourriel.
- Ils doivent retirer les adresses « soft » générant un message de non-livraison temporaire (4xx : Échecs isolés) lorsque le nombre total de refus est supérieur à 5 lors de campagnes consécutives à partir d'une seule liste ou totalise 5 à partir de plusieurs listes en 10 jours.

Les politiques de traitement des messages de non-livraison sont expliquées en détails sur les sites suivants :

- **http://help.yahoo.com/help/us/mail/defer**
- **www.isipp.com/standards.php**
- **http://postmaster.info.aol.com/guidelines/bestprac.html**

3. Les pixels espions (éléments en HTML cachés) et les avis de réception sont des façons inexactes de déterminer les statistiques de taux d'ouverture des envois des campagnes. Les expéditeurs sont vivement encouragés à cesser de les utiliser et à adopter d'autres mesures de la performance.

Les pixels espions sont des mesures de l'efficacité des campagnes de marketing par courriel extrêmement inexactes et leur usage est déconseillé.

Les pixels espions ne sont plus fiables pour plusieurs raisons, mais surtout à cause des changements techniques apportés aux principaux logiciels d'envoi de courriel (par exemple dans le cadre de ses mesures de sécurité anti-virus, Outlook ne les téléchargera plus par défaut et ne les affichera pas dans le panneau de prévisualisation). De plus, les clients utilisent de plus en plus souvent un logiciel anti-virus qui, par défaut, interdit le téléchargement des pixels espions.

On déconseille également le recours aux éléments d'images d'un pixel sur un pixel, blanc sur blanc pour mesurer les taux d'ouverture. On recommande plutôt d'utiliser les parcours des usagers sur des adresses URL codées, enchâssées et d'autres méthodes de mesure des actions des abonnés (par exemple rendement des investissements, actes d'achat).

Les expéditeurs qui entendent utiliser les pixels espions devraient se familiariser avec les implications pour la vie privée soulevées, notamment, dans l'étude publiée par la Network Advertising Initiative (**www.networkadvertising.org/Web_Beacons_11-1-04.pdf**) et respecter les modalités qui y sont énoncées.

À l'heure actuelle, la rétention des abonnés — soit le nombre de personnes qui continuent de s'abonner après chaque courriel — est une des mesures les plus utiles pour évaluer la réussite d'un programme de courriels. Clairement, l'objectif est de ne pas avoir de désabonnements, ce qui indiquerait que l'organisme fournit un contenu en temps voulu, pertinent et apprécié. À leur tour, ces avantages fidéliseront la clientèle et gagneront sa confiance — un atout pour n'importe quel organisme.

Exemple de lettre de conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques*

Nom de la liste : _____

En qualité de chef de file des services de publipostage, la **SociétéABC** est fière de son engagement à l'égard de la protection de la vie privée des consommateurs et de la conformité aux lois applicables, notamment à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Par conséquent, nous profitons de l'occasion pour mettre à jour les renseignements que nous avons au sujet de la liste susmentionnée.

Un examen de la LPRPDE et du respect de la vie privée des consommateurs
La LPRPDE porte uniquement sur les dossiers des consommateurs (destinés à une adresse domiciliaire). La loi affirme, entre autres choses, que les consommateurs inscrits sur une liste doivent avoir consenti à la collecte de leurs renseignements personnels et à leur communication à des tiers à des fins de marketing ou de communication. En outre, en vertu de la loi, les options de retrait offertes aux consommateurs doivent être mises en vigueur avant que leur nom soit communiqué à des fins de marketing.

Ce dont nous avons besoin
Il arrive de plus en plus souvent que les expéditeurs demandent des renseignements à propos des messages de confidentialité utilisés par les propriétaires de listes. Nous devons conserver les renseignements suivants dans nos dossiers pour assurer l'expédition rapide des commandes.

Veuillez fournir un spécimen du formulaire de consentement ou de retrait que vous utilisez présentement. Nous en conserverons un exemplaire dans nos dossiers à titre de référence aux fins d'usage éventuel et répété de cette liste.

Veuillez cocher une des cases ci-après, puis signer, dater et renvoyer ce document à l'attention de la **SociétéABC** au numéro de télécopieur (XXX) XXX-XXXX. Veuillez communiquer avec notre département des XXXXXXXXX au (XXX) XXX-XXXX ou à **info@societeABC.com** si vous avez des questions.

[ ] Je garantis et je fais valoir que cette liste EST CONFORME à la LPRPDE. Mon organisation a obtenu le consentement de tous les consommateurs inscrits sur cette liste pour recueillir leurs renseignements personnels et les communiquer à des tiers à des fins de marketing ou de communication, et a veillé à ce que les options de retrait soient mises à la disposition des consommateurs avant que leur nom ne soit communiqué à des fins de marketing. Mon organisme observera toutes les lois provinciales ou fédérales portant sur la protection des renseignements personnels pouvant entrer en vigueur à compter d'aujourd'hui, dans la mesure où elles s'appliquent aux renseignements personnels recueillis, utilisés ou communiqués par lui.

[ ] Je garantis et fais valoir que cette liste N'EST PAS CONFORME à la LPRPDE. Mon organisme n'a pas obtenu le consentement de tous les consommateurs inscrits sur cette liste pour recueillir leurs renseignements personnels et les communiquer à des tiers à des fins de marketing ou de communication, et/ou n'a pas veillé à ce que les options de retrait soient mises à la disposition des consommateurs avant que leur nom ne soit communiqué à des fins de marketing.

APPENDICE D

TROIS CONSEILS IMPORTANTS POUR LUTTER CONTRE LE POURRIEL

Les pourriels sont des courriels non sollicités, généralement de nature commerciale, annonçant un produit ou un service, qui diffusés massivement à des milliers d'adresses de courriel à la fois, inondent les boîtes de réception. Il ne s'agit pas d'un courriel commercial légitime auquel le consommateur a consenti. Le pourriel est souvent un véhicule pour la fraude, les virus et les documents à contenu offensant.

Le pourriel est un problème d'envergure qui fait perdre beaucoup de temps et d'argent aux consommateurs, aux entreprises et au gouvernement. Chacun doit faire sa part pour se protéger et protéger les autres du pourriel. Le **Groupe de travail canadien sur le pourriel** a formulé trois conseils pour vous aider à vous protéger et à lutter contre le pourriel.

Arrêtez le pourriel ici : trois conseils clés

1. Protégez votre ordinateur

Le pourriel est une source croissante de virus informatiques. Il est essentiel que vous protégiez votre ordinateur contre les messages transportant des virus. Installez un logiciel anti-virus et anti-pourriel et mettez-le à jour régulièrement. Procurez-vous aussi la protection supplémentaire d'un coupe-feu.

2. Protégez votre adresse de courriel

Réservez une adresse de courriel pour les contacts personnels et professionnels en qui vous avez confiance. Créez une adresse de courriel extensible distincte pour d'autres utilisations en ligne.

3. Protégez-vous

N'essayez rien, n'achetez rien et ne répondez pas aux pourriels. Supprimez-les. C'est une bonne façon de ne pas en recevoir d'autres dans l'avenir.

1. Protégez votre ordinateur

Protégez votre ordinateur avec des logiciels anti-pourriel et anti-virus et autres logiciels de protection.

Les logiciels anti-pourriel peuvent vérifier automatiquement vos courriels pour détecter les pourriels avant qu'ils ne parviennent à votre boîte de réception, et les envoient à la poubelle. Vous ou un membre de votre famille ne risquez donc plus d'ouvrir accidentellement un pourriel, et vous pouvez gérer vos courriels de façon plus efficace.

Pour vous protéger contre les pourriels et les pièces jointes contenant des virus, installez des correctifs de sécurité et des programmes anti-virus dans votre système d'exploitation et mettez-les à jour régulièrement.

Un coupe-feu procure une protection supplémentaire contre le piratage informatique et protège vos renseignements personnels.

N'entrez jamais en ligne sur un ordinateur non protégé contre les pourriels et les virus et dépourvu de coupe-feu.

Vérifiez toujours la source.

N'ouvrez jamais de pièce jointe, sauf si vous en attendez d'une personne sûre. Un polluposteur peut s'emparer du compte courriel d'un particulier ou d'une entreprise (processus appelé « mystification ») pour transmettre un virus à votre ordinateur. Si vous avez des soupçons au sujet d'une pièce jointe, vérifiez sa provenance auprès de l'expéditeur avant de l'ouvrir.

Ne laissez pas votre ordinateur devenir un zombie.

Sans les moyens de protection proposés dans le présent document, votre ordinateur risque d'être infecté par un virus programmé pour créer une passerelle (techniquement appelée « passerelle proxy ») qui transmet le pourriel à d'autres destinataires. Dans les cas graves, votre FSI pourrait être obligé de fermer votre compte. La réparation d'un ordinateur infecté peut coûter des centaines, voire des milliers de dollars.

Quand vous terminez une séance en ligne, vous devriez sortir d'Internet et éteindre votre ordinateur. De plus en plus, les polluposteurs transmettent les pourriels au moyen d'ordinateurs domestiques non protégés dotés d'une connexion Internet haute vitesse, pour les utiliser comme zombies.

2. Protégez votre adresse de courriel

Gérez les risques de connexion en ligne.

Utilisez des adresses de courriel distinctes pour vos différentes activités en ligne : créez une adresse de courriel que vous communiquez *seulement* aux relations personnelles et professionnelles sûres. Créez des adresses de courriel extensibles pour d'autres activités. Si vos adresses de courriel sont inondées de pourriels, supprimez-les.

Choisissez une adresse de courriel composée d'une combinaison de lettres et de chiffres. Une adresse de courriel complexe empêche les polluposteurs de découvrir votre compte courriel facilement en se servant d'un logiciel qui combine les noms et prénoms de façon aléatoire.

Restez discret.

L'affichage de votre adresse de courriel partout dans Internet attirera les pourriels. Donnez votre adresse de courriel *uniquement* aux personnes que vous connaissez et à qui vous faites confiance.

Un polluposteur recueille des adresses de courriel à l'aide de logiciels divers, comme les robots de recherche qui parcourent Internet pour trouver des adresses de courriel et les ajouter à leurs listes.

Si vous êtes inondé de pourriels, changez d'adresse de courriel.

3. Protégez-vous

Supprimez-le, tout simplement!

Pas d'essai! Pas d'achat! Pas de réponse! Ne visitez jamais les sites Web annoncés dans un pourriel et n'achetez jamais le produit ou service annoncé. Un pourriel est presque toujours frauduleux. *Supprimez-le, tout simplement!*

Ne répondez pas.

Il ne faut jamais ouvrir un pourriel, y répondre ou cliquer sur le lien « supprimer » ou « désabonner ». Cela confirme votre adresse de courriel, et vous recevrez encore plus de pourriels!

Ne mordez pas à l'hameçon d'un polluposteur. Protégez vos données personnelles.

Un polluposteur peut s'emparer de vos données personnelles en pratiquant « l'hameçonnage » (pêche aux données personnelles). Voici comment. Vous recevez un courriel provenant d'une source fiable avec qui vous faites affaire, comme une banque ou une cyberentreprise. Souvent, ce courriel prétend que vous devez absolument fournir des données personnelles, comme votre nom d'utilisateur, votre mot de passe et même le numéro de vos cartes de crédit. Il arrive aussi qu'on menace de bloquer votre compte si vous ne fournissez pas ces renseignements. Le lien Web qui est alors indiqué vous dirige vers un faux site bien imité. Sachez qu'une entreprise ne communique JAMAIS de cette manière avec ses clients. Si vous avez des soupçons, appelez l'entreprise concernée pour vérifier si le courriel est légitime. Ne répondez jamais à ce genre de courriel et n'entrez pas dans un site par le lien inclus dans un pourriel que vous soupçonnez de pratiquer l'hameçonnage. Si un site Web vous intéresse, consultez-le directement à l'aide d'un navigateur Web.

APPENDICE E

RAPPORTS COMPLÉMENTAIRES ET DOCUMENTS DE TRAVAIL

Les documents suivants présentent de la documentation complémentaire sur les travaux du Groupe de travail sur le pourriel et les conclusions des sous-groupes. On peut consulter ces documents à l'adresse : **www.e-com.ic.gc.ca**.

Ouvrages généraux

- Sommaire des commentaires reçus, Avis publié dans la *Gazette du Canada* concernant le *Plan d'action anti-pourriel pour le Canada*
- Groupe de travail sur le pourriel : Table ronde des intervenants clés
- Sommaire des contributions au Forum en ligne de consultation publique du Groupe de travail sur le pourriel

Documents des sous-groupes

- Aperçu des technologies anti-pourriel
- Document de conception de la Base de données canadienne sur les pourriels
- Document d'accompagnement des *Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux*
- Conclusions du Sous-groupe de travail sur l'examen de la législation et son application

Documents d'information

- Un droit privé d'action prévu par la loi contre les polluposteurs au Canada
- Évaluation de la certification du courriel
- Vue d'ensemble du problème du pourriel acheminé sur les appareils sans fil au Canada
- Propositions concernant le Centre canadien de lutte contre le pourriel
- Comparaison internationale des mesures anti-pourriel

GLOSSAIRE

Adresse de courriel *(Email address)*
Nom identifiant l'expéditeur ou le destinataire d'un courriel. L'adresse prend la forme de **boiteauxlettres@dom.ain**, où **dom.ain** est un nom de domaine consultable dans le DNS, et **boiteauxlettres** est un identifiant arbitraire utilisé par le gestionnaire du domaine pour identifier un internaute.

Adresse IP *(IP address)*
Adresse numérique utilisée pour identifier de manière unique un ordinateur ou autre appareil connecté à Internet. Une adresse IP se compose d'habitude d'une série de quatre nombres décimaux séparés par des points, comme 168.0.1.10.

Adresse URL *(URL)*
Chaîne de caractères normalisés servant à identifier une page Web ou une autre ressource en ligne. Prend habituellement la forme **http://www.mondomaine.ca/unepage**.

Attaque de dictionnaire *(Dictionary attack)*
Technique servant à deviner les adresses de courriel. L'arnaqueur essaie de livrer du courriel à un grand nombre d'adresses fictives, utilisant des termes tirés d'un dictionnaire ou des combinaisons de lettres, par exemple **aaaa@exemple.ca**, **aaab@exemple.ca**, ou **zzzz@exemple.ca**.

Attaque par déni de service *(Denial of service attack - DoS ou DOS)*
Attaque informatique destinée à empêcher un serveur ou réseau d'opérer en noyant son trafic. Par exemple, un arnaqueur pourrait envoyer des milliers de courriels à un serveur de courrier, dans le but de le submerger et de l'empêcher de distribuer les courriels. Les attaques peuvent frapper les serveurs de courrier, les serveurs Web, les serveurs DNS et les routeurs de réseaux. Le pourriel en vrac peut causer une attaque par déni de service.

Base de données WHOIS *(WHOIS)*
Service Internet utilisé pour demander des renseignements sur les domaines et les réseaux d'Internet. N'a pas été universellement mise en œuvre.

Blocage du port 25 *(Port 25 blocking)*
Théoriquement, chaque ordinateur sur Internet a la capacité technique d'envoyer du courrier à un autre ordinateur. En pratique, la majorité des internautes envoient leur courriel au destinataire final par l'entremise du serveur de leur FSI. Ces dernières années, la majorité du courrier envoyé directement (plutôt que par un FSI) a été du pourriel et des virus. Bon nombre de FSI empêchent maintenant leurs clients d'envoyer leur courrier directement, exigeant que celui-ci soit acheminé par le truchement de leur serveur où ils peuvent filtrer les virus et prendre d'autres mesures contre les abus. Comme le protocole de contrôle de transmission (TCP) attribue un numéro de port à chaque service, et que le courriel est expédié par le port 25, les FSI procèdent ainsi au blocage du port 25.

Le blocage du port 25 pour les usagers du réseau commuté et les abonnés à large bande constitue une pratique exemplaire.

Cheval de Troie *(Trojan Horse)*
Programme qui, en plus de sa fonction nominale, accomplit secrètement une deuxième fonction.

Clefs de domaine *(Domain keys)*
Technologie proposée par Yahoo!® qui ajoute aux messages une signature cryptographique identifiable par les destinataires. Elle permet de vérifier si le message provient du domaine de l'expéditeur du courriel et s'il a été modifié en transit.

Collecte *(Harvesting)*
Abrégé de « collecte d'adresses »

Collecte d'adresses *(Address harvesting)*
Action de recueillir des adresses de courriel automatiquement à partir de sites Web et d'autres sources en ligne.

Compte fonctionnel *(Role account)*
Compte de courriel devant être établi et maintenu par tous les secteurs ayant une connectivité Internet, conformément à la série de documents Request for Comments (RFC) de l'Internet Engineering Task Force (IETF). De tels comptes comprennent **postmaster@sampledomain.ca**, **abuse@sampledomain.ca** et **hostmaster@sampledomain.ca**.

Consentement actif *(Opt-in)*
Également appelé « consentement explicite » ou « positif ». Selon cette forme de consentement, que l'on appelle généralement le « consentement explicite », l'organisme offre à la personne concernée la possibilité d'accepter l'utilisation proposée. À moins que la personne ne prennent des mesures pour consentir à l'utilisation prévue – en d'autres mots, dire « oui » – l'organisme ne présumera pas que le consentement a été donné. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Consentement implicite *(Implied consent)*
Selon le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation, « le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement ». Cela comprend les situations où l'utilisation ou la communication prévue est évidente compte tenu du contexte, et où l'organisme peut présumer avec peu ou pas de risque que la personne, en fournissant les renseignements personnels, est consciente de l'utilisation ou de la communication prévue et y consent. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Courriel de marketing *(Marketing email)*
Courriel principalement destiné à annoncer la disponibilité de produits ou services. Comparer avec « courriel transactionnel ».

Courriel transactionnel *(Transactional email)*
Courriel contenant des renseignements sur des transactions commerciales courantes ou antérieures, notamment confirmation d'une vente, numéro d'enregistrement, facture ou confirmation de consentement actif ou de refus. Comparer avec « courriel de marketing ».

Défaillance passagère *(Transient failure)*
Brève défectuosité survenant de façon irrégulière et imprévue.

DNS
Système de noms de domaine, le système qui permet aux utilisateurs de localiser les ordinateurs sur Internet au moyen des noms de domaine. Les serveurs DNS maintiennent une base de données des noms de domaine (c'est-à-dire noms de l'hôte) et de leurs adresses IP correspondantes. Par exemple, si le nom **www.macompagnie.ca** était présenté à un serveur DNS, l'adresse IP 204.0.8.51 pourrait être retournée. Le DNS inclut plusieurs types de données, notamment les fichiers A pour adresses IP et les inscriptions d'échange de courriel (MX) des serveurs de courrier.

Le DNS est réparti entre de nombreux serveurs dont la plupart délèguent la responsabilité des noms à d'autres serveurs. Dans l'exemple qui précède, l'Internet Assigned Numbers Authority (IANA), organe responsable de la gestion de l'ensemble du système DNS, déléguerait tout les **.ca** à l'Agence canadienne d'enregistrement Internet (ACEI). Celle-ci déléguerait tous les **.macompagnie.ca** au déposant de ce nom et ce dernier exploiterait à son tour les serveurs qui ont l'information concernant **www.macompagnie.ca**.

Domaine *(Domain)*
Un nom utilisé sur Internet. Les domaines Internet sont formés de sections multiples séparées par des points comme **ic.gc.ca** ou **www.macompagnie.com**.

En-tête *(Header)*
Dans un courriel, partie initiale du message composée d'une série de lignes le décrivant. Chaque ligne commence par une étiquette comme « De : » ou « Sujet : » afin de déterminer sa signification. L'en-tête est suivi d'un espace vierge, puis du corps du message.

Filtre *(Filters)*
Logiciel qui distingue le courriel voulu du courriel non voulu à l'aide des caractéristiques du message. Par exemple, il peut vérifier la présence de certaines chaînes de textes, les tendances textuelles approchées, les ressemblances avec d'autres messages ou autres critères.

Fournisseur de services de courriel *(ESP or email service provider)*
Société qui offre des services de courriel aux autres entreprises. Ce sont, notamment, la collecte et le maintien des listes d'adresses de courriel, l'envoi de courriel en vrac aux adresses figurant sur les listes, le retrait des adresses qui génèrent des messages de non-livraison et le traitement des plaintes et des rapports d'abus concernant les envois.

Hameçonnage *(Phishing)*
L'hameçonnage est une tentative d'escroquerie basée sur l'usurpation d'identité d'une personne ou d'une organisation de confiance, dans le but de voler des renseignements personnels. Par exemple, l'envoi d'un faux courriel utilisant l'identité d'une institution financière, dans lequel on demande aux destinataires de visiter un site Web pour confirmer leurs coordonnées bancaires, site qui est en fait contrôlé par un pirate.

HTML
Langage de balisage de texte, ce système de codage permet de formater les pages Web et les courriels formatés. HTML utilise des balises de texte comme <h2>A Topic</h2> qui indique un en-tête de deuxième niveau et important text, un texte en caractères gras.

Identification de l'expéditeur *(Sender ID)*
Un schéma d'authentification, semblable à SPF, parrainé par Microsoft. Voir « SPF ».

Identité EHLO/HELO *(EHLO/HELO identity)*
Nom utilisé par l'ordinateur d'envoi pour s'identifier à l'ordinateur de réception au début de chaque transaction SMTP. Pour fournir son nom d'identification, l'ordinateur d'envoi se sert de la commande dite EHLO ou HELO.

Ligne de mention objet *(Subject line)*
Ligne faisant partie de l'en-tête d'un courriel. Les programmes de courriel affichent toujours la ligne de mention objet dans la liste des messages. La description exacte du contenu sur la ligne de mention objet est considérée comme une pratique exemplaire.

Liste blanche *(White list)*
Liste contenant les adresses courriel ou IP qui seront automatiquement acceptées par le serveur de courrier. Elle peut être utile en faisant partie d'un système de vérification par un filtre anti-pourriel. Comparer à « liste noire ».

Liste noire *(Black list)*
Liste contenant les adresses IP, adresses de courriel ou noms de domaine dont les courriels ne sont pas acceptés. La forme la plus courante est une liste noire de système de noms de domaine (DNSBL), une liste d'adresses IP distribuée par l'entremise du DNS d'Internet. Les listes noires de DNSBL les plus connues sont la Spamhaus Black List (SBL), la Composite Black List (CBL) et la liste noire DNSBL originale, appelée Mail Abuse Prevention System (MAPS) Reverse Black List (RBL). Comparer avec « liste blanche ».

Logiciel espion *(Spyware)*
Logiciel qui contient un programme espion et qui emploie à l'arrière plan la connexion Internet de l'utilisateur pour recueillir et transmettre, à son insu et sans sa permission, des données personnelles et modifier le fonctionnement de son ordinateur. À titre d'exemples : les logiciels de surveillance des claviers, qui envoient à un tiers une liste des touches sur lesquelles un utilisateur a appuyé, et les logiciels publicitaires affichant des annonces publicitaires choisies par leur propriétaire.

Maliciel, ou programme pirate *(Malware)*
Terme générique désignant les logiciels hostiles, tels virus, vers et chevaux de Troie.

Manœuvre frauduleuse de l'Afrique de l'Ouest, arnaque 419 ou fraude du Nigeria *(West African 419 or Nigerian scam)*
Fraude axée sur le paiement d'une commission escomptée, selon laquelle une personne prétendant représenter un pays d'Afrique de l'Ouest demande à la victime de l'aider à soutirer d'importantes sommes d'argent d'un compte gouvernemental. Également appelée arnaque 419, d'après le numéro de l'article de la loi nigérienne qui l'interdit.

Avant de déménager en Afrique, elle était connue sous le nom de *Spanish Prisoner* et remonte sous cette forme aux années 1600.

Messagerie texte *(Text messaging)*
Courts messages comportant du texte plutôt que des images. Ils sont accessibles instantanément (messagerie instantanée) ou par l'entremise d'un téléphone mobile.

MI ou messagerie instantanée *(IM or instant messaging)*
Messages de texte livrés immédiatement de l'ordinateur de l'expéditeur aux destinataires. Les systèmes de MI comprennent AOL® Instant Messenger™, Yahoo!® Messenger et MSN® Messenger.

Mouchard, ou témoin *(Cookie)*
Petit fichier créé et stocké dans l'ordinateur de l'internaute par un serveur Web. C'est une façon pour les sites Web d'identifier l'utilisateur d'un site, de connaître ses habitudes de navigation et de le reconnaître lors de ses visites subséquentes. L'historique d'un utilisateur permet aux concepteurs de sites Web d'adapter dynamiquement le contenu des pages Web et de créer des expériences individualisées pour l'internaute. Selon la programmation du serveur Internet, il peut contenir des renseignements personnels tels que des mots de passe de sites et des numéros de compte.

Les mouchards internes émanent du site Web visité, tandis que les mouchards tierce partie émanent généralement des sources de publicité sur le site visité. Ils permettent au publicitaire de déterminer si l'internaute visite plusieurs sites Web qui affichent ses annonces, posant ainsi un risque sur le plan de la sécurité.

Les navigateurs Web modernes permettent de refuser tous les mouchards, les mouchards tierce partie ou les mouchards de sites Web désignés.

Mystification, ou usurpation d'adresse IP *(Spoofing)*
Technique qui consiste à usurper l'identité d'une autre personne ou organisation, ce qui permet de faire croire que le courriel provient d'une source différente de la source véritable.

Parcours *(Clickstream)*
Séquence des requêtes ou de clics effectués par un internaute lors de la visite d'un site Web. Sur un site Web commercial, le parcours peut inclure une consultation du catalogue, le placement d'articles dans un panier virtuel, la transmission de renseignements sur le paiement et l'expédition et le passage de la commande.

Pixel invisible *(Web bug)*
Également appelé pixel espion, il s'agit d'une image GIF (graphics interchange format) invisible. C'est une façon pour l'expéditeur d'un courriel en HTML de déterminer si et quand le destinataire a ouvert le message et l'a lu.

Port 587 ou SUBMIT *(Port 587 or SUBMIT)*
Port de rechange que de nombreux services de courriel offrent à leurs clients pour l'envoi du courriel au serveur du FSI. L'authentification de l'expéditeur étant exigée avant l'envoi, la vérification du courriel expédié par SUBMIT est plus facile que sur le port 25. SUBMIT est également appelé port 587 car ce dernier lui est associé.

Pourriel *(Spam)*
Il n'y a pas de définition universellement acceptée du pourriel, mais de nombreux pays le considèrent comme étant un courriel commercial diffusé massivement sans le consentement explicite des destinataires.

rDNS ou DNS inversé *(rDNS or reverse DNS)*
Système de noms de domaine inversé, service servant à retracer un nom de domaine à partir d'une adresse IP. Il effectue la fonction inverse du système de retraçage DNS habituel. Le système DNS inversé sert souvent à consigner les messages entrants selon leur nom de domaine à des fins statistiques et de vérification. L'exactitude du rDNS constitue une pratique exemplaire pour les ordinateurs clients et les serveurs.

Refus *(Opt-out)*
Également appelé « consentement négatif ». L'organisme offre à la personne concernée l'occasion de se prononcer en désaccord avec une utilisation proposée. À moins que la personne ne prenne des mesures pour exprimer un consentement négatif à l'égard de l'utilisation prévue – en d'autres mots, dire « non » – l'organisme présume que le consentement a été donné et exécute l'utilisation prévue. La personne devrait être clairement informée que, en omettant d'exprimer son refus, elle consent à ce que les renseignements soient utilisés aux fins proposées. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Relation d'affaires existante *(Existing business relationship)*
Une relation d'affaires existe lorsque :
1) le destinataire s'est procuré un produit ou service auprès d'un organisme au cours des 18 derniers mois;
2) le destinataire n'a pas indiqué qu'il souhaitait se retirer de la liste d'envoi des courriels commerciaux ou promotionnels ni autrement interrompu la relation.

Un affilié ou un tiers ne peut se fier à la relation d'affaires antérieure d'un autre organisme pour envoyer des courriels commerciaux ou promotionnels.

Réseau d'ordinateurs zombies *(Botnet)*
Réseau de « zombies » qui sont utilisés pour envoyer du pourriel dans un autre but. Un seul réseau comprend souvent des centaines ou des milliers d'ordinateurs.

Retour à l'envoyeur *(Bounces)*
Procédé de rejet d'une tentative de livraison d'un courriel. Un courriel retourné à l'expéditeur indique que le courriel précédent n'a pu être livré.

En cas de non-livraison temporaire « soft bounce », l'ordinateur expéditeur peut tenter de livrer le message plus tard. La non-livraison permanente « hard bounce » reflète un échec.

Une boîte aux lettres d'arrivée pleine, un serveur surchargé ou d'autres problèmes temporaires peuvent causer une non-livraison temporaire. La non-livraison permanente indique généralement qu'une adresse est invalide ou que l'hôte a pour politique de rejeter le courrier en provenance de l'expéditeur.

Serveur *(Server)*
Ordinateur qui fournit un ou plusieurs services aux autres ordinateurs, comme le serveur de courriel, le serveur DNS et le serveur Web.

SMTP
« Simple Mail Transfer Protocol », système utilisé pour envoyer un message d'un ordinateur à l'autre dans Internet. Le protocole SMTP est défini dans la série de documents Request for Comments (RFC 2821) de l'Internet Engineering Task Force.

SPF

« Sender Policy Framework », une extension du protocole SMTP dans Internet. SPF vérifie la légitimité d'un courriel en comparant le domaine du courriel de l'expéditeur contre une liste d'ordinateurs autorisés à envoyer des courriels à partir de ce domaine. Pour de plus amples renseignements, voir **http://spf.pobox.com**.

Usurpation d'identité *(Identity theft)*

L'utilisation de renseignements personnels volés pour usurper l'identité de quelqu'un en vue de commettre une fraude. Le vol peut être commis dans le but d'accéder à des comptes bancaires réels, d'obtenir des prêts bancaires ou à d'autres fins frauduleuses.

Vente croisée *(Cross-sell)*

Vente où l'on encourage le client à acheter un produit ou service associé à un produit ou service déjà acheté. Comparer avec « vente de gamme supérieure ».

Vente de gamme supérieure *(Up-sell)*

Vente où l'on offre à un client un article ou un produit ou service plus cher. Comparer avec « vente croisée ».

Ver *(Worm)*

Programme pirate qui se propage directement en se copiant sur d'autres ordinateurs grâce à des défauts de sécurité dans les logiciels informatiques. Le premier ver utilisait un défaut de sécurité dans les systèmes Solaris de Sun Microsystem et les systèmes VAX, mais les vers actuels exploitent les défauts inhérents à Microsoft Windows. Comparer avec « virus ».

Virus

Programme pirate qui se propage en s'attachant à une autre ressource sur un ordinateur. Les premiers virus se propageaient en s'attachant aux programmes d'application, mais les virus actuels se propagent par l'entremise du courriel. Comparer avec « ver ».

Zombie

Ordinateur infecté par un pirate et contrôlé à distance par le créateur, le distributeur ou le contrôleur de ce pirate. À l'heure actuelle, la majeure partie du pourriel est envoyée au moyen de zombies.

NOTES